UNITED STATES DISTRICT COURT
DISTRICT OF PUERTO RICO

NAICOM CORPORATION, et al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	No. 3:21-cv-01405-JAW
	)	
DISH NETWORK CORPORATION, et al.,	)	
	)	
Defendants.	)	

ORDER ON THE DISH/NAGRASTAR DEFENDANTS' MOTION TO DISMISS

Two limited liability companies and several of their employees file a motion to dismiss plaintiffs' seven-count complaint, arising out of a criminal investigation wherein the private parties assisted federal law enforcement. The Court grants the motion to dismiss, dismissing all seven counts. The Court dismisses plaintiffs' RICO claims because plaintiffs have not adequately pleaded the existence of an enterprise, a pattern of racketeering activity, or a conspiracy. The Court dismisses plaintiffs' Computer Fraud and Abuse Act claim, Stored Communications Act claim, Digital Millennium Copyright Act claim, and Defend Trade Secrets Act claim because, taking plaintiffs' allegations as true, the private entities' assistance to law enforcement fell within statutory exceptions for authorized law enforcement activity. Finally, the Court dismisses the Puerto Rico Uniform Trade Secrets Act claim because plaintiffs have not adequately alleged that the defendants misappropriated their trade secrets.

I. PROCEDURAL HISTORY

On August 27, 2021, Naicom Corporation, D&V IP Holdings, LLC, Paylink, LLC, and Kiaras, LLC, filed a seven-count complaint against approximately twenty

known Defendants and two dozen unknown Defendants.[1] *Compl.* (ECF No. 1). The Court has twice permitted Plaintiffs to amend their complaint, and the Second Amended Complaint is now the operative complaint. *Am. Compl.* (ECF No. 100); *Second Am. Compl.* (ECF No. 130).

The parties categorize the numerous Defendants into four groups: 1) DISH Network LLC, NagraStar LLC, Bert Eichhorn, Emily Rinkel,[2] Jordan Smith, and Kevin Gedeon (the DISH/NagraStar Defendants); 2) DISH Network Corporation (DISH Corp. or DNC); 3) Toltec Investigations, LLC and its President and CEO, Michael Thomas Jaczewski (the Toltec Defendants); and, 4) former U.S. Attorney Rosa E. Rodriguez-Velez, former Assistant U.S. Attorney Jose Capo-Iriarte, Assistant U.S. Attorney Nicholas W. Cannon (the USAO Defendants) and Special Agents and employees of the Federal Bureau of Investigation Douglas Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, and Jason Lopez (the FBI Defendants) (collectively, the Federal Defendants).

Plaintiffs allege: (1) violations of the Racketeer Influenced and Corrupt Organizations Act (RICO); (2) a RICO conspiracy; (3) violations of the Computer Fraud and Abuse Act (CFAA); (4) violations of the Stored Communications Act (SCA);

---

[1] This is the second lawsuit arising out of the underlying events at issue. On August 25, 2020, a group of plaintiffs, including many of Plaintiffs here, filed a *Bivens* action against many of the same defendants. *See Quinones-Pimentel v. Cannon*, No. 3:20-cv-01443-JAW, 2022 U.S. Dist. LEXIS 48109, at *2-3 (D.P.R. Mar. 17, 2022). On March 17, 2022, the Court dismissed the plaintiffs' *Bivens* action. *Id.* at *88. The plaintiffs appealed, and the Court of Appeals for the First Circuit affirmed the Court's dismissal on October 27, 2023. *Quinones-Pimentel v. Cannon*, 85 F.4th 63, 66-68 (1st Cir. 2023).

[2] In their Second Amended Complaint, Plaintiffs use the spelling, "Rinkle." *See, e.g.*, *Second Am. Compl.* ¶ 43. In her filings, however, Ms. Rinkel uses the spelling, "Rinkel." *See, e.g.*, *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel, and Jordan Smith's Mot. to Dismiss* at 1. No doubt, Ms. Rinkel knows how to spell her own name, and the Court uses "Rinkel" throughout this order.

(5) violations of the Digital Millennium Copyright Act (DMCA); (6) violations of the Defend Trade Secrets Act (DTSA) by misappropriation of trade secrets; and (7) violations of the Puerto Rico Industrial and Trade Secrets Protection Act (PTSA) under the Uniform Trade Secrets Act (Law No. 80). *Second Am. Compl.* ¶¶ 124-202.

On October 31, 2022 and November 1, 2022, each of the four groups of Defendants filed a motion to dismiss the complaint. *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel, and Jordan Smith's Mot. to Dismiss* (ECF No. 134) (*Defs.' Mot.*); *Def. DISH Network Corp.'s Mot. to Dismiss* (ECF No. 136); *Defs.' Toltec Investigations, L.L.C. and Mike Jaczewski's Mot. to Dismiss* (ECF No. 137); *Fed. Defs.' Mot. to Dismiss* (ECF No. 138).

On December 5, 2022, Plaintiffs filed a response to the DISH/NagraStar Defendants' motion to dismiss. *Mot. in Resp. to Dish/NagraStar Defs.' Mot. to Dismiss* (ECF No. 147) (*Pls.' Opp'n*). On January 18, 2023, Plaintiffs responded to the Federal Defendants' motion. *Mot. in Resp. to the Fed. Defs.' Mot. to Dismiss* (ECF No. 153). On February 21, 2023, the Toltec Defendants withdrew a section of their motion to dismiss, *Unopposed Notice of Partial Withdrawal of Toltec Investigations L.L.C. and Mike Jaczewski's 12(b)(2) Mot. to Dismiss* (ECF No. 163), and on February 27, 2023, Plaintiffs responded to the remainder of the Toltec Defendants' motion. *Mot. in Resp. to Toltec Investigations and Mike Jaczewski's Mot. to Dismiss* (ECF No. 167). On March 17, 2023, Plaintiffs responded to DISH Corp.'s motion. *Mot. in Resp. to Dish Network Corp.'s Mot. to Dismiss* (ECF No. 179).

Each group of Defendants filed a reply in support of its motion. *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel, and Jordan Smith's Reply* (ECF No. 164) (*Defs.' Reply*); *Fed. Defs.' Reply* (ECF No. 173); *Defs. Toltec Investigations L.L.C. and Michael Jaczewski's Reply in Supp. of Rule 12(b)(6) Mot. to Dismiss* (ECF No. 185); *DISH Network Corp.'s Reply in Supp. of Its Mot. to Dismiss* (ECF No. 196).

Finally, Plaintiffs filed sur-replies opposing each motion. *Sur-Reply to the Dish Network, LLC and NagraStar, LLC Reply Mot. to Pls.' Resp. to Defs.' Mot. to Dismiss SAC* (ECF No. 182) (*Pls.' Sur-Reply*); *Sur-Reply Mot. to Fed. Defs.' Reply Mot. to Pls.' Resp. to Fed. Defs.' Mot. to Dismiss, SAC* (ECF No. 190); *Sur-Reply Mot. to the Toltec Investigations L.L.C. and Michael Jaczewski's Reply Mot. to Pls.' Resp. to Their Mot. to Dismiss SAC* (ECF No. 195); *Sur-Reply Mot. to Dish Network Corp.'s Reply Mot. to Pls.' Resp. to Mot. to Dismiss SAC* (ECF No. 199).

II. FACTS[3]

A. The Parties

In 2015 and 2016, Darwin Quinones-Pimentel and Victor Vega-Encarnacion founded Naicom Corporation (Naicom) and D&V IP Holdings, LLC (D&V) to offer Internet Protocol Television (IPTV) services. The companies are structured such that D&V holds the proprietary "intellectual technology" created by Mr. Quinones, and

[3] Consistent with Federal Rule of Civil Procedure 12(b)(6), in describing the facts, the Court has relied upon the allegations in the Plaintiffs' Second Amended Complaint. *Foley v. Wells Fargo Bank, N.A.*, 772 F.3d 63, 68 (1st Cir. 2014); *Medina-Velázquez v. Hernández-Gregorat*, 767 F.3d 103, 108 (1st Cir. 2014) ("We examine whether the operative complaint states a claim for which relief can be granted when we construe the well-pleaded facts in the light most favorable to the plaintiffs, accepting their truth and drawing all reasonable inferences in plaintiffs' favor" (internal citation omitted)).

Naicom licenses the technology from D&V to distribute television programming. *Second Am. Compl.* ¶ 63. Kiaras, LLC (Kiaras) and Paylink, LLC (PayLink) are also joint ventures operated by Mr. Quinones and Mr. Vega. *Id.* ¶ 14. Kiaras is a human resources and time-and-attendance management company, and PayLink is a payroll processing company. *Id.* Both Kiaras and Paylink operate on the "PAYLINK AND KIARAS Cloud Network," another proprietary intellectual technology creation of Mr. Quinones. *Id.* ¶¶ 5-6. All four companies are corporations existing under the laws of the commonwealth of Puerto Rico with their places of business located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907. *Id.* ¶¶ 33-36.

DISH Network Corporation (DISH Corp. or DNC) was organized in 1995 as a corporation under the laws of the State of Nevada, started offering the DISH® branded pay-tv service in March 1996, and is the nation's third largest pay-tv provider. *Id.* ¶ 37. DISH Network LLC (DISH LLC) was organized in 1987 as a Limited Liability Corporation under the laws of the state of Colorado. *Id.* ¶ 38.

NagraStar, LLC (NagraStar) is a joint venture between DISH Corp. and Kudelski SA formed in 1998. *Id.* ¶ 39. NagraStar's focus is delivering and maintaining security solutions for satellite and Internet-based television systems and other connectivity initiatives in North America, and their mission also includes anti-piracy investigations and cooperation with law enforcement agencies. *Id.* Jordan Smith was at all relevant times a Manager of Field Security & Investigations and Senior Anti-Piracy Investigator for NagraStar. *Id.* ¶ 41. Bert Eichhorn and Emily

Rinkel were Managers of Field Security & Investigations for NagraStar. *Id.* ¶¶ 42-43. Kevin Gedeon was a Manager of Fraud Investigations for NagraStar. *Id.* ¶ 44.

Toltec Investigations, LLC (Toltec) is a private investigative agency specializing in investigating the technology and distribution involved in IPTV systems, copyrights, patents, and "Trademark and Brand's Intellectual Property." *Id.* ¶ 40. Michael Thomas Jaczewski, a.k.a. Brian Parsons, was at all relevant times President and Chief Executive Officer of Toltec. *Id.* ¶ 45.

Rosa Emilia Rodriguez-Velez was at all relevant times the United States Attorney for the District of Puerto Rico. *Id.* ¶ 46. Jose Capo-Iriarte was an Assistant U.S. Attorney (AUSA) and head of the office's Criminal Division. *Id.* ¶ 47. Nicholas Cannon was an AUSA and Deputy Chief of the Cybercrimes Division. *Id.* ¶ 48.

Douglas Leff was at all relevant times Special Agent in Charge of the FBI's San Juan Division. *Id.* ¶ 49. Also in that division, Brad Rex was a Supervisory Special Agent, Lance Lange, Kevin Pearson, and Clay Rehrig were Special Agents, Juan Galarza a Computer Science Officer, and Jason Lopez an Evidence Technician. *Id.* ¶¶ 50-55.

B. Naicom's Origins

Between 2002 and 2012, Mr. Quinones developed the intellectual technology, including the source code, underpinning the Paylink and Kiaras Cloud Workforce Management system and Naicom's IPTV services. *Id.* ¶ 5. The proprietary IPTV system was characterized as a Dynamic Internet Semantic Multicast Environment (DISME), which "enabled for the first time the broadcast of media via private networks and the internet, a new concept of IPTV service to distribute Live-Video

Television Content (media) to residences, business, and primes customers." *Id.* ¶¶ 8-11.

By 2016, Mr. Quinones had completed all DISME technology alpha and beta tests and, alongside Mr. Vega, founded Naicom. *Id.* ¶ 12. Naicom is a network and internet communication platform that delivers live television, video on-demand content, internet, and wireless network services to subscribers worldwide. *Id.* Naicom also provides instant access to television shows, movies, and music/videos on-demand, and live sports and music events through Naicom's set-top box using IPTV and TV Everywhere (TVE) on any mobile device. *Id.*

Mr. Quinones and Mr. Vega registered Naicom as a closed corporation with the State Department of Puerto Rico and complied with all requirements as a legitimate IPTV business. *Id.* ¶ 66. Naicom also requested to manufacture its own brand of set-top boxes for end users through Informir LLC and acquired the programing licenses to distribute on-demand content in the United States, Puerto Rico, and the U.S. Virgin Islands through worldwide television network companies. *Id.* ¶¶ 67-68. In 2017, Naicom became a member of the National Rural Telecommunications Cooperative (NRTC). *Id.* ¶ 68.

On January 6, 2017, Naicom submitted a request to the Apple Corporation to have its TV App added to Apple's AppStore. *Id.* ¶ 69. Apple's legal department requested that Naicom produce all licenses authorizing the distribution of programming to Naicom's subscribers via Naicom's TV App. *Id.* On February 16, 2017, Apple approved Naicom's App for inclusion in the Apple AppStore. *Id.* ¶ 70. In

December 2017, Sam's Club approved Naicom to launch and distribute Naicom's IPTV set-top box in their retail stores. *Id.* ¶ 71.

C. Naicom's Information Security

Naicom went to great lengths to protect its intellectual technology. *Id.* ¶¶ 64-65. D&V IP Holdings and Naicom developed significant amounts of confidential and proprietary information, including non-public information relating to the DISME's source codes, patterns, formulas, algorithms, methods, and techniques; the technological vision for Naicom's IPTV content, distribution, marketing, servicing, research and development efforts and strategies; business and marketing performance strategies; financial data and business plans; technical data; customer development management programs; and subcontractor and vendor relationships (collectively, with the DISME, the Confidential Information or Naicom's Confidential Information). *Id.* ¶ 64.

To protect this information, Plaintiffs only installed on their servers, located at the Naicom Data Center Facility, what is known as compiled executable. *Id.* ¶ 65. The entire system was installed with an operating system that allowed the hard drive to be encrypted and, to access the servers, an authorized employee would need to enter the secure data facility and provide a username and password. *Id.* The server is not exposed to the internet and could only be accessed from inside the facility. *Id.* The Confidential Information was also downloaded onto a hard disk and kept in a safe box. *Id.*

Plaintiff companies took additional steps to safeguard their confidential information and proprietary data, including restricting employee access, requiring

employees to execute non-disclosure agreements, imposing restrictions on remote access, and implementing encryption. *Id.* ¶¶ 72-76.

D. Negotiations with Claro Puerto Rico

In 2017, Naicom entered into negotiations with Claro Puerto Rico[4] (Claro) to distribute Naicom set-top boxes to Claro customers. *Id.* ¶ 77. Claro represented to Naicom that it had approximately 320,000 internet subscribers who received only five megabytes and thus could not subscribe to Claro's IPTV services, which required sixty megabytes to upload programming. *Id.* ¶ 78. During negotiations, Naicom and Claro entered into a mutual non-disclosure agreement prior to discussing and analyzing business information and the contents of the resellers' agreement. *Id.* ¶ 79. Claro's Product Development Officer, Anibal Rios, projected that the Claro-Naicom business alliance would bring in over $10,000,000 in monthly gross revenue for the first year and over $13,000,000 for the second year only taking into account Claro's corporate and residential subscribers in Puerto Rico. *Id.* ¶ 80. Naicom projected that the Claro-Naicom alliance would add 100,000 new corporate subscribers, plus another 150,000 residential subscribers, bringing in projected monthly gross sales of $9,000,000 in the first year and $12,000,000 in the second year. *Id.* ¶ 81.

Claro had an existing contract with DISH Network Satellite TV, whereby DISH Network provided TV programming to Claro's internet subscribers who could

[4] Presumably because Claro Puerto Rico is a well-known business in Puerto Rico, the Second Amended Complaint does not describe Claro Puerto Rico except by name. *See Second Am. Compl.* ¶ 68. According to Wikipedia, Claro Puerto Rico is the one of the largest telecommunications companies in Puerto Rico. *See Claro P.R.*, WIKIPEDIA (updated Oct. 14, 2023), *https://en.Wikipedia.org/wiki/Claro_Puerto_Rico.*

not subscribe to Claro's IPTV services. *Id.* ¶ 82. The Naicom deal represented a cancellation threat to DISH Network's contract with Claro. *Id.* Claro was also considering shutting down its IPTV business division due to loss of revenue. *Id.* During the negotiations for the Claro-Naicom deal, Carlos Garcia, Claro's IPTV business manager, became privy to information that the Claro-Naicom deal would leave him jobless if Claro opted to shut down its IPTV division, which he managed. *Id.* ¶ 83. Mr. Garcia alerted DISH Network that the Claro-Naicom IPTV deal would lead to cancellation of the DISH contract with Claro, which Plaintiffs allege led to "great animosity" between DISH Network and Naicom. *Id.* ¶ 84. On August 14, 2018, after a year of meetings between Naicom and Claro, Claro pulled out of negotiations without notice. *Id.* ¶ 85. Plaintiffs believe the DISH Network Defendants advised Claro to withdraw because the FBI was investigating Naicom and its founders. *Id.* ¶ 86.

E. The DISH Network Investigation

On August 7, 2017, the DISH/NagraStar and DISH Corp. Defendants instructed the Toltec Defendants to purchase two Naicom TV set-top-box receivers so that the Defendants[5] could reverse engineer Plaintiffs' intellectual technology. *Id.* ¶ 87. The Defendants conducted "sniffing" to determine the direction of Naicom TV traffic and locate Naicom's facility. *Id.* The Defendants also used sniffing to attack and penetrate Naicom's servers and computers, monitoring content and capturing

[5] Plaintiffs often refer in the Second Amended Complaint to the "Association in Fact defendants." *See, e.g., id.* ¶ 87. As the Court interprets Plaintiffs' complaint, this term refers to all Defendants collectively. *See id.* ¶¶ 17, 62 (listing all the Defendants as together "form[ing] an Association in Fact").

information on the network under the supervision of the Federal Defendants. *Id.* One of the two set-top box receivers was maintained by the DISH/NagraStar Defendants, the other by the Toltec Defendants. *Id.* ¶ 88. Both receivers were used for the attacks on Naicom's data center servers. *Id.*

Mr. Jaczewski purchased the two set-top boxes from Naicom under the false name of "Brian Parsons," and he provided false contact information. *Id.* ¶ 89. According to the Defendants, their investigation revealed that the receiver provided access to approximately forty-three channels, including Disney, TBS, ESPN, CNN, HBO, Showtime, and Cinemax. *Id.* ¶ 90. The Defendants downloaded the Naicom TV App through the Apple AppStore, which provided access to approximately forty-two channels, and tested Naicom TV several times to determine whether it was providing DISH programming. *Id.* The tests revealed no DISH content. *Id.*

The Defendants also contacted several media companies to inquire into whether Naicom had the appropriate licensing contracts to distribute its programming. *Id.* ¶ 91. On each occasion, the investigators were informed that Naicom was authorized to distribute the network's content. *Id.* The investigators also discovered that Naicom's TV distribution technology was a threat to DISH Network and Sling TV, representing future competition for subscribers in Puerto Rico and the United States. *Id.* ¶ 92.

The DISH/NagraStar Defendants informed the other Defendants that they could not penetrate Naicom's Data Center computers and servers remotely, and thus direct, physical access would be required to extract Naicom's intellectual property.

Id. ¶ 93. They knew that by entering the data center and shutting down the computers and servers, they would be able to bypass Naicom's security measures and access the internal hard drive. *Id.* ¶ 94.

According to Naicom, the Defendants knew that the intellectual property was extremely valuable and worth obtaining by any means necessary to advance their own television programming distribution system, and the Defendants conspired to misappropriate the technology for economic advantage. *Id.* ¶ 95.

The DISH/NagraStar Defendants thereafter filed a complaint with the Federal Defendants alleging that Naicom was running an IPTV pirate operation. *Id.* ¶ 98. Plaintiffs allege that the motive behind the complaint was to secure NagraStar and DISH Network's participation in a search of Naicom's Data Center and the seizure of Naicom's computers, servers, and other hardware containing Naicom's intellectual property and trade secrets, under the ruse of assisting the Federal Defendants in discovering incriminating evidence. *Id.* Acquiring this information has given the DISH/NagraStar Defendants a competitive advantage over Naicom. *Id.* ¶ 99.

F. The Executions of the Search Warrants

1. The First Search of Naicom's Data Center

On August 27, 2019, the Federal Defendants applied for two search warrants: one for Naicom Corporation located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907, and the other for Naicom's Data Center located at Villa Fontana, 4SS N2 Via Josefina, Carolina, Puerto Rico. *Id.* ¶¶ 19, 33, 105. Plaintiffs allege that the search warrants were "issued under illegal and

unlawful means" because the Federal Defendants provided affidavits they knew to contain false and perjured information. *Id.* ¶ 20.

On August 27, 2019, the Federal and DISH/NagraStar Defendants executed the warrants, with the DISH/NagraStar Defendants "acting as federal agents." *Id.* ¶ 21. They seized documents, hard drives, and thumb drives, and downloaded data from the computers and servers containing Plaintiffs' Confidential Information. *Id.* Plaintiffs allege that the Defendants knew from their investigation prior to the searches that Naicom was authorized to distribute its programming and was not pirating content. *Id.* ¶ 101. The Defendants also allegedly knew that the evidence collected in the Federal Defendants' investigative files "negated any criminal wrongdoing that Naicom's founders were committing the crimes charged in the search and seizure warrant affidavit and application." *Id.* ¶ 102.

At the conclusion of the August 27, 2019 search, the Federal Defendants "learned that Naicom TV counted with all the programming distribution contract and agreements"[6] and instructed Mr. Quinones and Mr. Vega to report to the FBI offices with their licensing contracts for an interview. *Id.* ¶ 103. This interview took place with the Federal Defendants sitting at one table and the DISH/NagraStar Defendants sitting at another table, allegedly posing as federal agents. *Id.* ¶ 104. The Defendants questioned Mr. Quinones about how Naicom acquired the IPTV distribution contracts and the technology used to distribute the programing. *Id.*

[6] Here, the Court quotes the language in the Second Amended Complaint. *Second Am. Compl.* ¶ 103. In the context of this sentence, the meaning of the verb, "counted," is unclear. It would make more sense if the sentence used "complied with," rather than "counted." Whichever verb is correct, however, makes no difference in the Court's ruling on the motion to dismiss.

They also inspected Naicom's contracts with content providers, which contained trade/business secrets and confidential information regarding DISME technology. *Id.*

2. The Second Search of Naicom's Data Center

On August 29, 2019, U.S. Attorney Rodriguez-Velez and AUSAs Capo-Iriarte and Cannon instructed FBI Agents Lange and Pearson to return to Naicom's data center with DISH/NagraStar Defendants Smith, Gedeon, and Eichhorn. *Id.* ¶ 105. Naicom alleges that the USAO Defendants ordered this search despite knowing beforehand that Naicom was a legitimate business and there was no probable cause for continued investigation. *Id.* Without obtaining new warrants, the Defendants again entered Naicom's data center facility, performed password resets, and installed "pen drives and other electronic instruments" to bypass security measures and download and seize Naicom's Confidential Information. *Id.* ¶¶ 22, 106. The agents used keys taken from Naicom's offices to enter Naicom's data center. *Id.* ¶ 105.

During the search, Agent Pearson contacted Naicom employee Jaime Echevarria and ordered him to come to the Data Center, as Agent Pearson wanted to speak with him, Mr. Quinones, and Mr. Vega. *Id.* ¶ 107. Upon arriving at the Data Center, Mr. Quinones observed Agents Lange and Pearson allowing Mr. Smith, Mr. Gedeon, and Mr. Eichhorn to access Naicom's Data Center computers, servers, and other hardware equipment without authorization from Naicom. *Id.* ¶ 108.

During the search, Agents Pearson and Lange pressured Mr. Quinones to sign a hold-harmless document accepting that he had run a pirate operation in the past so that they could close the case. *Id.* ¶ 109. Otherwise, they threatened that they

would shut down the Data Center operation. *Id.* Mr. Quinones refused, despite Agents Pearson and Lange imploring him to sign the document. *Id.* ¶ 110.

Sometime thereafter, Mr. Vega arrived and, upon entering the Data Center, asked Agents Pearson and Lange if they had another search warrant to enter and search the Data Center. *Id.* ¶ 111. Agent Lange represented to Mr. Vega that the search warrant gave him ten days to come in and out and search the Data Center. *Id.* Mr. Vega told Agent Lange that Agent Lange was violating the United States Constitution and Federal law. *Id.*

Mr. Vega thereafter informed Agents Pearson and Lange that he had discovered via LinkedIn that the alleged FBI experts who executed the search and interrogated Mr. Quinones and him at the FBI offices were Kevin Gedeon, investigator for DISH Network, and Jordan Smith, Bert Eichhorn, and Emily Rinkel, investigators for NagraStar. *Id.* ¶ 112. Mr. Vega questioned Agents Lange and Pearson as to why the FBI brought in his competition to search, inspect, and photograph private documents and allowed them access to computers and servers containing trade secrets, code sources, and business and intellectual property belonging to Naicom. *Id.* ¶ 113. Mr. Vega called his attorney and told him about the second search. *Id.* ¶ 114. After speaking with Agent Lange, the FBI agents and DISH/NagraStar investigators shut down Naicom's business operation and left the premises. *Id.*

G. The Demand for the Return of Property Under Rule 41(g)

On September 6, 2019, Plaintiffs filed a motion to demand the return of seized property under Rule 41(g) of the Federal Rules of Criminal Procedure. *Id.* ¶ 115. The

District Court granted the Plaintiffs' Rule 41(g) motion on November 5, 2019, noting that the Government had waived objections to the court's Report & Recommendation. *Id.* ¶¶ 116-17.

H. Plaintiffs' Alleged Harm

Plaintiffs allege that the criminal investigation caused significant damage to their business reputation and unfairly enriched their competitors. *Id.* ¶¶ 118-19. They allege that prior to the execution of the search warrants, they had a great reputation and were about to close on a $15,000,000 investment deal, but investors pulled out upon learning Naicom was under criminal investigation. *Id.* ¶¶ 120-21. Plaintiffs also allege that Naicom was about to close a multimillion-dollar deal with Claro when Claro learned of the FBI's investigation and pulled out of negotiations. *Id.* ¶ 122. Plaintiffs say they have lost subscribers because of negative publicity resulting from the investigation and that the Defendants' intrusion into Naicom's Data Center computers, servers, and equipment caused damage leaving subscribers without TV programming services for several weeks and cost more than $500,000 to repair. *Id.* ¶ 123.

I. Plaintiffs' Causes of Action

The Plaintiffs bring seven counts. Count One alleges that the Defendants violated RICO by forming an association in fact to advance the criminal objective of stealing Plaintiffs' intellectual property and trade secrets by committing mail and wire fraud, among other crimes. *Id.* ¶¶ 124-53.

Count Two alleges that the Defendants engaged in a RICO conspiracy by conspiring to plan and execute the scheme outlined in Count One. *Id.* ¶¶ 154-57.

Count Three alleges that the Defendants the CFAA by accessing Naicom's computer systems without authorization or in excess of authorization and obtaining and using valuable information from those computers. *Id.* ¶¶ 158-68.

Count Four alleges that the Defendants violated the SCA by "willfully and intentionally access[ing] without authorization a facility which operates servers, encoders, computers, and telecommunications systems and technology, by electronically transmitting communications involved in Webservers, Email-Servers, Carrier Grade Routers which interconnected with local ISP providers through Border Gateway Protocols (BGP) in exchanging routing information between autonomous systems." *Id.* ¶¶ 169-75.

Count Five alleges that the Defendants violated the DMCA by illegally obtaining Plaintiffs' copyright-protected software programs, documents, confidential information, and research. *Id.* ¶¶ 176-84.

Count Six alleges that the Defendants violated the DTSA by stealing Plaintiffs' trade secrets, including DISME technology, intellectual property, and other confidential information. *Id.* ¶¶ 185-94.

Finally, Count Seven alleges that the Defendants misappropriated Plaintiffs' trade secrets in violation of the PTSA. *Id.* ¶¶ 195-202.

III. THE PARTIES' POSITIONS

A. The DISH/NagraStar Defendants' Motion to Dismiss

The DISH/NagraStar Defendants urge the Court to dismiss Plaintiffs' complaint for eight reasons: 1) "Plaintiffs' factual allegations assert neither a constitutional nor statutory violation under RICO, thus their claims are barred by

qualified immunity"; 2) "the DISH/NagraStar Defendants, acting as alleged federal agents, lacked the criminal intent to engage in racketeering activity"; 3) "the *Noerr-Pennington* doctrine bars Plaintiffs' RICO claims"; 4) "Plaintiffs' RICO claims are predicated upon a legal impossibility, as the United States is the proper defendant and has not waived sovereign immunity"; 5) the Second Amended Complaint "fails to satisfy the essential elements of a RICO claim under [18 U.S.C.] § 1962(c)"; 6) Plaintiffs' "RICO conspiracy claim under [18 U.S.C.] § 1962(d) fails without a viable substantive claim and is otherwise inadequately pled"; 7) Plaintiffs' "federal statutory claims cannot satisfy the 'without authorization' elements, are otherwise inadequately pled, and the conduct alleged is covered by immunity"; and 8) Plaintiffs' "PTSA claim is inadequately pled, the conduct complained of cannot fit within the scope of the 'improper means' element, and is otherwise subject to the Westfall Act." *Defs.' Mot.* at 2-3.

Leading with their qualified immunity argument, the DISH/NagraStar Defendants observe that "courts have consistently held that the qualified immunity doctrine provides a defense to civil RICO claims." *Id.* at 7-8 (citing *Gonzalez v. Otero*, 172 F. Supp. 3d 477, 508 (D.P.R. 2016); and *Gonzalez v. Lee Cnty. Hous. Auth.*, 161 F.3d 1290, 1300 (11th Cir. 1998)). They aver that, even though they are "private individuals," they are "entitled to the qualified immunity defense for the official misconduct alleged by Plaintiffs" because they were "'acting as federal agents' under color of federal law at the direction and supervision of the Federal Defendants." *Id.* at 8 (quoting *Second Am. Compl.* ¶¶ 21-22).

Next, the DISH/NagraStar Defendants argue that they "lacked the criminal intent to engage in 'racketeering activity.'" *Id.* at 9 (capitalization altered). According to the DISH/NagraStar Defendants, each of the alleged RICO predicate acts "[is] supported by allegations of legitimate government action." *Id.* (alteration in *Def.'s Mot.*) (quoting *Kahre v. Damm*, No. 2:07-CV-00231-DAE-RJJ, 2007 U.S. Dist. LEXIS 95978, at *26 (D. Nev. Dec. 18, 2007)). The DISH/NagraStar Defendants further emphasize that their assistance in the execution of the search warrants does not "render the warrants invalid or constitute illegal trespass, as federal law authorizes government officials to procure assistance from private individuals in aid of a search warrant's execution." *Id.* at 9-10. Finally, the DISH/NagraStar Defendants maintain that "the purchase of IPTV set top box receivers and related subscription services using a pseudonym as part of an undercover federal investigation to detect pirated IPTV content is not mail or wire fraud." *Id.* at 10.

Turning to their *Noerr-Pennington* argument, the DISH/NagraStar Defendants observe that "Plaintiffs' RICO claims are premised on the DISH/NagraStar Defendants' pre-indictment investigative activities conducted at the direction of, and in conjunction with, the Federal Defendants." *Id.* at 12-13. They argue that "[c]ourts applying the *Noerr-Pennington* doctrine have deemed such pre-litigation investigative activities to be necessary predicates to formal legal proceedings and, as such, protected conduct incidental to prosecution under the *Noerr-Pennington* doctrine." *Id.* at 13.

The DISH/NagraStar Defendants then discuss sovereign immunity. Although Plaintiffs purport to sue the Defendants in their individual capacities, the DISH/NagraStar Defendants urge the Court to regard this case as an official-capacity suit because the Second Amended Complaint "asserts RICO claims against the federal officials and DISH/NagraStar investigators, among others, complaining of actions taken by them in furtherance of official duties." *Id.* at 14. Moreover, the DISH/NagraStar Defendants contend that sovereign immunity bars Plaintiffs' RICO claims because "a suit against federal agencies or federal officials in their official capacity is essentially a suit against the United States," Plaintiffs ask for money damages, and Plaintiffs fail "to allege any unequivocal waiver of the federal government's sovereign immunity for their RICO claims and cannot evade the sovereign immunity bar here through artful pleading." *Id.* at 14-15.

Addressing Plaintiffs' RICO claims, the DISH/NagraStar Defendants first argue that "Plaintiffs cannot plead a cognizable RICO enterprise on the facts." *Id.* at 16 (capitalization altered). They maintain that "Plaintiffs still fail to allege plausible facts supporting the required structural features of an association-in-fact enterprise." *Id.* at 18. According to the DISH/NagraStar Defendants, their "alleged association with the Federal Defendants in carrying out law enforcement activities of investigative work and execution of search warrants does not give rise to a cognizable RICO enterprise and those claims must be dismissed." *Id.* at 18-19.

The DISH/NagraStar Defendants further maintain that "Plaintiffs cannot plead conduct of a criminal enterprise that is separate and apart from the conduct of

Defendants' own affairs." *Id.* at 19 (capitalization altered). They assert that "Plaintiffs fail to plead factual allegations establishing how the DISH/NagraStar Defendants took any part in the 'operation or management' of the alleged RICO enterprise," *id.* at 20 (quoting *Reves v. Ernst & Young*, 507 U.S. 170, 185 (1993)), and that "any contention that the DISH/NagraStar Defendants operated or managed the enterprise's affairs directly contradicts Plaintiffs' own allegations that the DISH/NagraStar Defendants acted 'as federal agents' under color of federal law at the direction and supervision of the Federal Defendants." *Id.* (quoting *Second Am. Compl.* ¶¶ 21-22).

In the DISH/NagraStar Defendants' view, Plaintiffs also "cannot plead a pattern of racketeering activity on the facts." *Id.* at 20 (capitalization altered). The DISH/NagraStar Defendants argue that the acts identified by Plaintiffs "are insufficient to establish predicate offenses under RICO or the continuity required to demonstrate RICO's pattern of racketeering activity." *Id.* They further conclude that the Second Amended Complaint "alleges no 'distinct threat of long-term racketeering activity,' real risk of 'future criminal conduct,' or predicate acts that 'are part of an ongoing entity's regular way of doing business,'" meaning that Plaintiffs have failed to allege the pattern of racketeering activity necessary to support a civil RICO claim. *Id.* at 21-22 (quoting *H.J. Inc. v. Nw. Bell Tel. Co.*, 492 U.S. 229, 242-43 (1989)).

Turning to Plaintiffs' RICO conspiracy claim, the DISH/NagraStar Defendants suggest this claim "fails for two independent reasons." *Id.* at 22. First, they contend that the RICO conspiracy claim must be dismissed because Plaintiffs failed to plead

a viable substantive RICO claim. *Id.* Further, they argue that "Plaintiffs' allegations of agreement and conspiracy are too vague and conclusory to state a claim for relief." *Id.*

Having fully addressed Plaintiffs' RICO claims, the DISH/NagraStar Defendants turn to the CFAA claim. According to the DISH/NagraStar Defendants, the Second Amended Complaint fails "to state a viable CFAA violation for two independent reasons: (i) accessing Plaintiffs' computers pursuant to a search warrant under color of federal law at the direction and supervision of the Federal Defendants does not constitute 'unauthorized access' or 'exceeding authorized access'; and (ii) Plaintiffs' claims of lost profits and trade secrets are not cognizable losses under the CFAA." *Id.* at 23-24. The DISH/NagraStar Defendants add that "Plaintiffs' assertion that the DISH/NagraStar Defendants harvested some malicious motive in aiding the Federal Defendants' execution of the search warrants . . . does not alter this analysis." *Id.* at 26 n.17 (citing *Van Buren v. United States*, 141 S. Ct. 1648, 1655 (2021)).

Similarly, the DISH/NagraStar Defendants contend that "Plaintiffs' SCA claim is legally untenable because . . . any wire or electronic communications purportedly accessed by the DISH/NagraStar Defendants, during the warrants' execution" are exempt from SCA liability under the statutory exceptions for law enforcement activity and good-faith reliance on a search warrant. *Id.* at 26-27. They put forth a similar argument with respect to Plaintiffs' DMCA claim, maintaining that their "conduct falls squarely within the DMCA's law enforcement activity exception and is exempt from liability." *Id.* at 28. Moreover, according to the DISH/NagraStar

Defendants, Plaintiffs' allegation that they "used password dumps under the direction and supervision of the Federal Defendants" is insufficient to trigger DMCA liability because "[t]hat conduct . . . does not constitute 'circumvention' for DMCA purposes." *Id.*

Finally, the DISH/NagraStar Defendants discuss Plaintiffs' DTSA and PTSA claims. They argue that their "conduct does not fall within the scope of conduct prohibited under the DTSA" because lawful means of acquisition are exempted from the statute. *Id.* at 29. Further, the DISH/NagraStar Defendants say that because their "purported acquisition of Plaintiffs' trade secrets represents either a lawful disclosure made in confidence to federal officials for the purpose of 'investigating a suspected violation of law,' or a 'lawful means of acquisition' conducted at the behest of federal officials in compliance with a search warrant, a cause of action under the DTSA is untenable." *Id.* at 30. Relatedly, the DISH/NagraStar Defendants assert that the PTSA claim fails because their conduct did not constitute "misappropriation," and Plaintiffs cannot satisfy the "improper means" requirement of the statute. *Id.* at 30-31.

The DISH/NagraStar Defendants conclude by asking the Court to dismiss all the claims in the Second Amended Complaint with prejudice because "any further amendments would be futile and further exhaust the resources of the Court, the Federal Defendants, and the DISH/NagraStar Defendants." *Id.* at 31-32.

B. Plaintiffs' Opposition

In response, Plaintiffs first argue that "the DISH/NagraStar Defendants are not entitled to qualified immunity from Plaintiffs' RICO claims." *Pls.' Opp'n* at 11.

According to Plaintiffs, the "special policy concerns involved in suing government officials" are "lacking" with respect to private parties. *Id.* at 13 (citing *Wyatt v. Cole*, 504 U.S. 158 (1992)). Even if private parties can invoke qualified immunity, Plaintiffs continue, "the proposed [Second Amended Complaint] also states the Dish/Nagrastar defendants' criminal and civil violations were clearly established and prohibited at the time they committed the crime." *Id.* at 14.

Plaintiffs then pivot to arguing that "the procurement of the issuance and execution of the search and seizure warrant and the subsequent warrantless search and seizure execution were illegal and unconstitutional." *Id.* at 18 (capitalization altered). They contend that the DISH/NagraStar Defendants and the Federal Defendants jointly procured search warrants that "contained materially false representations and perjured testimony," and ultimately lacked probable cause. *Id.* at 18-19. Additionally, Plaintiffs submit that "the alleged initial probable cause dissipated with the first search warrant execution," and thus the second search was "illegal and warrantless." *Id.* at 22.

Plaintiffs go on to argue that "the affidavit in support of the search warrant was defective on its face." *Id.* at 24 (capitalization altered). They contend that their computer systems were protected under the SCA, that the "conclusory" statements in the affidavit were insufficient to justify a search, and that the search ultimately did not comply with the SCA. *Id.* at 24-25. According to Plaintiffs, the Federal Defendants "did not seek authorization from the Magistrate to bring Plaintiffs' competitors, the Dish/Nagrastar defendants, to execute the search warrant," and

although Plaintiffs concede that 18 U.S.C. § 3105 allows private parties to assist in the execution of a search warrant, they counter that "the statute clearly prohibited the executing officer from bringing to the search a party which had another interest, profit, or other marketplace incentive." *Id.* at 28-29. Further, Plaintiffs submit that the DISH/NagraStar Defendants cannot rely on the search warrants to justify their actions because the Federal Defendants conceded the invalidity of the search warrants when they did not oppose Plaintiffs' motion for return of property under Federal Rule of Criminal Procedure 41(g). *Id.* at 30-32.

Shifting gears, Plaintiffs contend that "the *Noerr-Pennington* doctrine does not apply to the case at bar." *Id.* at 33 (capitalization altered). This is so, they continue, because the DISH/NagraStar Defendants' "grievance was a sham, knowingly assisted and carried out by the Federal defendants in order to gain access to Plaintiffs' premises and deprive them of their intellectual and trade secret property." *Id.* at 35-36. Plaintiffs maintain that the *Noerr-Pennington* doctrine "does not protect 'objectively baseless' sham litigation." *Id.* at 36.

Plaintiffs next argue that RICO does not contain any waiver of sovereign immunity. *Id.* at 36-37. They submit further that "the charges in this civil action were not brought against the United States, but against specific federal official/agents and the Dish/NagraStar defendants, in their individual and personal capacities, for criminal actions indictable under RICO, falling outside their scope of employment, and beyond their statutory authority," and thus, "Plaintiffs are allowed to prosecute under equitable civil remedies of the United States laws." *Id.* at 37.

Turning to the RICO counts, Plaintiffs submit that they have pleaded "a colorable RICO claim on the facts" because they have pleaded "enough facts in the [Second Amended Complaint to give] defendants a fair notice of what there is, and the grounds upon [which] they rest." *Id.* at 37-38 (capitalization altered). They add that they have also "pleaded a cognizable RICO enterprise on the facts." *Id.* at 39-41 (capitalization altered).

Plaintiffs further maintain that they have sufficiently "pleaded conduct of a criminal enterprise that is separate and apart from the conduct of Defendants' own affairs." *Id.* at 41 (capitalization altered). In their view, the three required elements for establishing a RICO enterprise are: 1) "an ongoing organization, formal or informal"; 2) that "the various associate[s] function as a continuing unit"; and 3) that the enterprise exists "separate and apart from the pattern of activity in which it engages." *Id.* at 42 (quoting *United States v. Turkette*, 452 U.S. 576, 583 (1981)). Plaintiffs assert that while they "will ultimately need to establish each of these factors, at this early juncture it is sufficient to merely [] allege the existence of an association-in-fact enterprise." *Id.* (quoting *Pappa v. Unum Life Ins. Co. of Am.*, No. 3:07-cv-0708, 2008 U.S. Dist. LEXIS 21500, at *29-30 (M.D. Pa. Mar. 18, 2008)). They add that it is reasonable to infer from the Second Amended Complaint that "the Association in Fact defendants functioned as a continuing unit and had an ascertainable structure distinct from that inherent in the conduct of a pattern of racketeering activity." *Id.* at 44.

Plaintiffs argue that they have established a pattern of racketeering activity because they have "pleaded that the Association in Fact defendants committed over 30 racketeering acts ranging from Mail and Wire fraud to theft of trade secrets, in a period of two years which began in July 2017 and ended in August 2019." *Id.* at 46. In their view, these "facts satisfied the closed period of repeated conduct," and there are also "allegations of a threat of continued activity, in reference to the Dish Network and Nagrastar corporation joint venture." *Id.* at 46-47.

Plaintiffs submit further that they have pleaded a viable RICO conspiracy claim because 18 U.S.C. § 1962(d) "criminalizes an agreement rather than any substantive criminal offense," meaning that "an agreement to associate with and participate in a yet-to-be formed racketeering enterprise that would affect interstate commerce constitutes a completed offense under § 1962(d)." *Id.* at 48-49 (citing *Salinas v. United States*, 522 U.S. 52, 62 (1997)). Plaintiffs therefore conclude that a substantive RICO claim is not required for a viable RICO conspiracy claim, although they maintain they have adequately alleged a substantive RICO claim. *Id.* at 49-50.

Turning to their CFAA claim, Plaintiffs first argue that they do not need to satisfy the heightened pleading requirements of Federal Rule of Civil Procedure 9(b). *Id.* at 50. They then reiterate their view that the DISH/NagraStar Defendants cannot rely on the search warrants because the government, in failing to oppose Plaintiffs' motion for return of property, conceded that the warrants were invalid. *Id.* at 51-52. Further, Plaintiffs maintain that they have demonstrated cognizable losses under the

CFAA because they "allege they incurred damages and loss in excess of $5,000 as a proximate result of Defendants' conduct." *Id.* at 53.

Plaintiffs similarly argue that the DISH/NagraStar Defendants cannot rely on the warrants as a defense to the SCA claim because "the Magistrate did not authorize access into Plaintiffs' electronic communications" pursuant to the SCA. *Id.* at 55. They then argue that they have satisfied the first and second elements of a SCA claim. *Id.* at 58-63. In particular, with respect to the second element, Plaintiffs maintain that the second search of the Data Center was a trespass, and "[p]ermission to access a stored communication does not constitute valid authorization if it would not defeat a trespass claim in analogous circumstances." *Id.* at 59-61.

Briefly addressing their DMCA claim, Plaintiffs argue that the DISH/NagraStar Defendants' motion should be denied for the "same factual and legal reasons" that apply to Plaintiffs' CFAA and SCA claims. *Id.* at 63-64.

Finally, Plaintiffs address their DTSA and PTSA claims. *Id.* at 64-68. They maintain that they have pleaded all the elements of a viable DTSA claim and urge the Court to "find that it is likely Plaintiff will be able to demonstrate a present and ongoing threat to its trade secrets." *Id.* at 66-67. According to Plaintiffs, "the DTSA authorizes relief even in cases of threatened misappropriation," and, regardless, the Second Amended Complaint demonstrates that the DISH/NagraStar Defendants misappropriated their trade secrets. *Id.* at 67-68. Plaintiffs suggest that because they adequately pleaded their DTSA claim, their PTSA claim must also survive because the standards under both statutes are the same. *Id.* at 64-65.

C. The DISH/NagraStar Defendants' Reply

The DISH/NagraStar Defendants begin by reiterating that Plaintiffs' RICO claims are barred by qualified immunity. *Defs.' Reply* at 2-4. They submit further that the Federal Defendants did not waive qualified immunity by failing to oppose the motion for return of property, arguing that "the Federal Defendants were not required to raise the qualified immunity defense in that proceeding to preserve their defense," and the Federal Defendants "did not make any concessions concerning the qualified immunity defense." *Id.* at 2-3.

Next, the DISH/NagraStar Defendants argue that Plaintiffs' reliance on the "sham" exception to *Noerr-Pennington* immunity "is misplaced." *Id.* at 5. This is so, they continue, because "a magistrate judge found probable cause sufficient to issue search warrants based on the petitioning conduct." *Id.* at 6. The DISH/NagraStar Defendants further aver that "Plaintiffs cannot dispute that the DISH/NagraStar Defendants' petitioning conduct was to procure legitimate government action to halt what they believed to be infringement and circumvention of copyrighted content." *Id.* at 6. Therefore, the DISH/NagraStar Defendants maintain that their "alleged petitioning activities prompting the government's investigation into Plaintiffs' infringing conduct can hardly be said to have been a sham." *Id.* at 7.

Turning to the elements of Plaintiffs' RICO claims, the DISH/NagraStar Defendants assert that "Plaintiffs make no attempt to detail the structure of the alleged RICO enterprise." *Id.* at 8. In their view, the allegations in the Second Amended Complaint "indicate neither the mechanics of a cohesive organization nor the efforts of a collaborative, decision-making operation guiding the enterprise's

misdeeds." *Id.* at 10. The DISH/NagraStar Defendants further reiterate that their "alleged association with the Federal Defendants to carry out legitimate law enforcement activity simply cannot constitute a cognizable RICO enterprise and the RICO claim must be dismissed." *Id.*

The DISH/NagraStar Defendants then submit that an additional reason for dismissal of the Second Amended Complaint is that "Plaintiffs plead no factual allegations establishing how the DISH/NagraStar Defendants took any part in the 'operation or management' of the alleged RICO enterprise and do not identify, which, if any, DISH/NagraStar Defendant, had a role in 'directing' the alleged enterprise's affairs." *Id.* at 11.

Similarly, the DISH/NagraStar Defendants argue that "Plaintiffs fail to plead any actionable predicate offenses much less a pattern of racketeering activity." *Id.* (capitalization altered). They contend that "Plaintiffs rely on dicta in *Bellville v. Town of Northboro*, 375 F.3d 25, 32 (1st Cir. 2004)" to inaccurately claim "that the First Circuit issued guidelines governing law enforcement's use of civilians in aid of a warrant's execution and to imply that prior judicial approval is required before procuring civilian assistance." *Id.* at 13. Further, they maintain that "the 30+ online purchases made using a pseudonym as part of an undercover investigation to detect pirated IPTV content do no constitute mail fraud or wire fraud, but rather protected, pre-indictment petitioning activities." *Id.* at 14.

Briefly addressing Plaintiffs' RICO conspiracy claim, the DISH/NagraStar Defendants urge dismissal because "Plaintiffs do not allege facts demonstrating that

any Defendant agreed to anything—much less that each of them consciously agreed to commit at least two predicate acts or understood the overall objective of the alleged enterprise and knowingly agreed to further its affairs or participate in an 'endeavor, which, if completed, would satisfy all the elements of a substantive [RICO] offense.'" *Id.* at 16 (quoting *United States v. Rodríguez-Torres*, 939 F.3d 16, 23 (1st Cir. 2019)).

Moving on to Plaintiffs' CFAA claim, the DISH/NagraStar Defendants reiterate that their actions were authorized pursuant to valid search warrants, and "Plaintiffs' contention that the search warrants were invalid does not vitiate the Federal Defendants or the DISH/NagraStar Defendants' 'authorized access.'" *Id.* at 16-17. The DISH/NagraStar Defendants further maintain that Plaintiffs "fail to satisfy the statutory damages requirement" and "their attempt to now proffer text messages and invoices in support of the same should be rejected." *Id.* at 17-18.

In a similar vein, the DISH/NagraStar Defendants argue that "because Plaintiffs' SCA claim is predicated upon the DISH/NagraStar Defendants' alleged access to Plaintiffs' computers during the Federal Defendants' execution of the search warrants, any wire or electronic communications purportedly accessed by the DISH/NagraStar Defendants falls within" enumerated statutory exceptions for law enforcement conduct or good-faith reliance on a search warrant. *Id.* at 18-19.

Turning to Plaintiffs' DMCA claim, the DISH/NagraStar Defendants suggest that Plaintiffs' opposition brief contains new allegations under the DMCA's anti-trafficking provisions. *Id.* at 19. "To the extent Plaintiffs seek to amend their [Second Amended Complaint] to advance an anti-trafficking claim," the DISH/NagraStar

Defendants continue, "their motion to amend should be denied." *Id.* Further, the DISH/NagraStar Defendants reiterate that Plaintiffs' DMCA claim should be dismissed because "the alleged conduct does not constitute 'circumvention'" and "it falls squarely within the DMCA's law enforcement activity exception." *Id.* at 20.

Finally, the DISH/NagraStar Defendants discuss Plaintiffs' DTSA and PTSA claims. *Id.* at 20-21. In their view, "Plaintiffs' DTSA claim does not plausibly plead misappropriation . . . because [the Second Amended Complaint] makes plain that rather than acquiring trade secrets by improper means, the DISH/NagraStar Defendants purportedly acquired them while 'acting as federal agents' under the direction and supervision of the Federal Defendants." *Id.* at 20 (quoting *Second Am. Compl.* ¶¶ 21-22). Additionally, the DISH/NagraStar Defendants argue their conduct "is otherwise exempt from liability under the lawful government activity provision or the immunized disclosure parameters." *Id.* The DISH/NagraStar Defendants aver that Plaintiffs' PTSA claim should be dismissed for similar reasons. *Id.* at 21.

D. Plaintiffs' Sur-Reply

In their sur-reply, Plaintiffs request that the Court reject or strike all the arguments in the DISH/NagraStar Defendants' reply that do not address a "new matter." *Pls.' Reply* at 1-2. Plaintiffs aver that the only "new matter" in the DISH/NagraStar Defendants' reply is the contention that Plaintiffs are trying to further amend their complaint to assert anti-trafficking claims under the DMCA. *Id.* at 2. Plaintiffs therefore ask the Court to disregard the remainder of the DISH/NagraStar Defendants' reply. *Id.* at 3-6. Further, Plaintiffs argue that their

Second Amended Complaint includes allegations pursuant to the anti-trafficking provisions of the DMCA. *Id.* at 6.

Plaintiffs conclude by asking the Court to deny the DISH/NagraStar Defendants' motion to dismiss because the Second Amended Complaint "sets forth a short and plain statement showing that they are entitled to relief" and to strike all the defenses raised by the DISH/NagraStar Defendants. *Id.* at 8-9.

IV. LEGAL STANDARD

Rule 12(b)(6) requires dismissal of a complaint that "fail[s] to state a claim upon which relief can be granted." FED. R. CIV. P. 12(b)(6). To state a claim, a complaint must contain, among other things, "a short and plain statement of the claim showing that the pleader is entitled to relief." FED. R. CIV. P. 8(a)(2). In other words, a complaint must contain "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp.* v. *Twombly*, 550 U.S. 544, 570 (2007)). A claim is facially plausible when "the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (citing *Twombly*, 550 U.S. at 556). Plausible means "'something more than merely possible' or 'merely consistent with a defendant's liability.'" *Germanowski v. Harris*, 854 F.3d 68, 71-72 (1st Cir. 2017) (internal citation omitted) (quoting *Schatz v. Republican State Leadership Comm.*, 669 F.3d 50, 55 (1st Cir. 2012)); *Ocasio-Hernández v. Fortuño-Burset*, 640 F.3d 1, 11 (1st Cir. 2011)). This is a "'context-specific' job that compels [judges] 'to draw on' [their] 'judicial experience and common sense.'" *Schatz*, 669 F.3d at 55 (quoting *Iqbal*, 556 U.S. at 679).

This is a "two-step analysis." *Cardigan Mountain Sch. v. N.H. Ins. Co.*, 787 F.3d 82, 84 (1st Cir. 2015). "First, the court must distinguish 'the complaint's factual allegations (which must be accepted as true) from its conclusory legal allegations (which need not be credited).'" *García-Catalán v. United States*, 734 F.3d 100, 103 (1st Cir. 2013) (quoting *Morales-Cruz v. Univ. of P.R.*, 676 F.3d 220, 224 (1st Cir. 2012)); *see also Schatz*, 669 F.3d at 55 (stating that a court may "isolate and ignore statements in the complaint that simply offer legal labels and conclusions or merely rehash cause-of-action elements"). "Second, the court must determine whether the factual allegations are sufficient to support 'the reasonable inference that the defendant is liable for the misconduct alleged.'" *García-Catalán*, 734 F.3d at 103 (quoting *Haley v. City of Boston*, 657 F.3d 39, 46 (1st Cir. 2011)).

V. DISCUSSION

A. Plaintiffs' Request to Strike the DISH/NagraStar Defendants' Reply

The Court begins by addressing Plaintiffs' argument that "the Court should either reject and/or strike from the Dish/NagraStar defendants' Reply any portion not addressing a new matter." *Pls.' Sur-Reply* at 1. Plaintiffs submit "that [upon] close examination[,] the Dish/Nagrastar defendants' factual argument and legal authorities[] did not contribute anything new that they had not already discussed in their [motion to dismiss], and their Reply is nothing more than a second response." *Id.* at 2.

The Court disagrees. Plaintiffs rely on District of Puerto Rico Local Civil Rule 7(c), which provides:

> With prior leave of court and within seven (7) days of the service of any objection to a motion, the moving party may file a reply, which shall not exceed ten (10) pages in length, and which shall be strictly confined to responding to new matters raised in the objection or opposing memorandum.

As this rule makes clear, a reply is proper so long as it addresses "new matters raised in the . . . opposing memorandum." *Id.*

Plaintiffs reason that the DISH/NagraStar Defendants' reply is noncompliant because it contains the same general arguments as their motion to dismiss. For example, Plaintiffs ask the Court to strike the reply's discussion of the *Noerr-Pennington* doctrine because "this issue was raised and discussed by the DISH/NagraStar Defendants in their [motion to dismiss]." *Pls.' Sur-Reply* at 4. But this reads Local Rule 7(c) too narrowly and the DISH/NagraStar Defendants' reply too strictly. The Court does not view Local Rule 7(c) as prohibiting a reply from expanding upon issues raised both in the original memorandum and the response so long as the response addressed the issue. *See Torres-Talavera v. Ford Motor Co.*, 965 F. Supp. 2d 220, 222 n.3 (D.P.R. 2013) (noting that, pursuant to Local Civil Rule 7(c), the plaintiffs' sur-reply was "confined to respond to the arguments made in defendant Ford's reply").

The Court's review of the reply's discussion of the *Noerr-Pennington* doctrine reveals that it focuses on Plaintiffs' argument, raised for the first time in their opposition brief, that the "sham" exception to the *Noerr-Pennington* doctrine applies. *See Defs.' Reply* at 4-7. The Court's further examination of the other supposedly recycled arguments in the DISH/NagraStar Defendants' reply yields similar results. While the DISH/NagraStar Defendants' reply discusses the same subject matter as

their motion to dismiss, the specific arguments in the reply are different and respond to the arguments in Plaintiffs' opposition brief. Therefore, the reply is proper under Local Civil Rule 7(c).

The Court denies Plaintiffs' request to strike.[7]

B. Plaintiffs' RICO and RICO Conspiracy Claims

To state a civil RICO claim under 18 U.S.C. § 1962(c), a plaintiff must allege four elements: (1) conduct; (2) of an enterprise; (3) through a pattern; (4) of racketeering activity. *Lerner v. Colman*, 26 F.4th 71, 77 (1st Cir. 2022) (citing *Sedima, S.P.R.L. v. Imrex Co.*, 472 U.S. 479, 496 (1985)). "Racketeering activity" is defined to include a variety of predicate offenses, including mail fraud, wire fraud, and theft of trade secrets. 18 U.S.C. § 1961(1). The civil-suit provision of the RICO statute grants the right to sue to "[a]ny person injured in his business or property by reason of a violation of" the substantive provisions of the statute. *Id.* § 1964(c).

Civil RICO claims "premised on mail or wire fraud must be particularly scrutinized because of the relative ease with which a plaintiff may mold a RICO pattern from allegations that, upon closer scrutiny, do not support it." *Efron v. Embassy Suites (P.R.), Inc.*, 223 F.3d 12, 20 (1st Cir. 2000). "[I]n cases alleging civil RICO violations, particular care is required to balance the liberality of the Civil Rules with the necessity of preventing abusive or vexatious treatment of defendants." *Miranda v. Ponce Fed. Bank*, 948 F.2d 41, 44 (1st Cir. 1991), *abrogated on other*

[7] Plaintiffs also suggest that the Court should strike all the defenses raised by the DISH/NagraStar Defendants under Federal Rule of Civil Procedure 12(f) because "there are no factual issues or issues of law to be resolved before the validity of the defenses in the present context may be determined." *Pls.' Sur-Reply* at 7-8. The Court declines to do so.

grounds by Salinas v. United States, 522 U.S. 52 (1997). "Civil RICO is an unusually potent weapon—the litigation equivalent of a thermonuclear device. The very pendency of a RICO suit can be stigmatizing and its consummation can be costly." *Id.* Accordingly, "courts should strive to flush out frivolous RICO allegations at an early stage of the litigation." *Figueroa Ruiz v. Alegria*, 896 F.2d 645, 650 (1st Cir. 1990).

1. RICO Enterprise

a. Legal Framework

In interpreting the RICO "enterprise" requirement, the Supreme Court has explained that "there is no restriction upon the associations embraced by the definition: an enterprise includes any union or group of individuals associated in fact." *Turkette*, 452 U.S. at 580. The enterprise concept is not unbounded, however, because an enterprise must be "an entity, for present purposes a group of persons associated together for a common purpose of engaging in a course of conduct." *Id.* at 583. In cases "involving an alleged associated-in-fact RICO enterprise, the existence of the charged enterprise does not follow, ipso facto, from evidence that those named as the enterprise's associates engaged in crimes that collectively may be characterized as a 'pattern of racketeering activity.'" *United States v. Cianci*, 378 F.3d 71, 81 (1st Cir. 2004).

Put differently, "criminal actors who jointly engage in criminal conduct that amounts to a pattern of 'racketeering activity' do not automatically thereby constitute an association-in-fact RICO enterprise simply by virtue of having engaged in the joint

conduct" and "[s]omething more must be found—something that distinguishes RICO enterprises from ad hoc one-time criminal ventures." *Id.* at 82. Ultimately, the First Circuit has "read *Turkette* to impose a requirement that those associated in fact function as an ongoing unit and constitute an ongoing organization. Also important to such an enterprise is that its members share a common purpose." *Id.* at 82 (internal quotations omitted). Finally, the existence of an enterprise "is proved by evidence of an ongoing organization, formal or informal, and by evidence that the various associates function as a continuing unit." *Turkette*, 452 U.S. at 583.

"Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice," *Iqbal*, 556 U.S. at 678, especially where "plaintiffs attempt to camouflage conclusory statements as allegations of fact." *A.G. ex rel. Maddox v. Elsevier, Inc.*, 732 F.3d 77, 81 (1st Cir. 2013).

b. Analysis

After sifting out Plaintiffs' conclusory statements, Court views the RICO allegations as pleaded as wafer thin, and the well-pleaded facts remaining are insufficient to establish that the alleged association in fact "function[ed] as an ongoing unit" or constituted an "ongoing organization." *Cianci*, 378 F.3d at 82 (internal quotations omitted).

As to the enterprise requirement, the Second Amended Complaint offers that, starting in 2017, all Defendants conspired at the outset and together "formed an Association in Fact, [including] Legal Entity Enterprises that would help the Association in Fact defendants advance the purpose and goals of the Racketeering

Enterprises' conspiratorial objectives in misappropriating themselves from Plaintiffs' DISME intellectual technology property, and trade secrets." *Second Am. Compl.* ¶¶ 17-18; *see also id.* ¶¶ 126-28. It adds that the "Association-In-Fact defendants knowingly agreed, combined, and conspired to conduct the affairs of the Racketeering Enterprise in attempting and committing theft of trade secrets through a hoax criminal investigation operation." *Id.* ¶ 155.

The Second Amended Complaint does assert that on August 7, 2017, Mr. Gedeon, Mr. Smith, Mr. Eichhorn, and Ms. Rinkel "instructed" Mr. Jaczewski to purchase a Naicom TV set-top-box receiver as part of an operation "supervised and approved" by the Federal Defendants. *Id.* ¶¶ 133-34. It also alleges that Mr. Gedeon, Mr. Smith, Mr. Eichhorn, and Ms. Rinkel subsequently "supervised and approved" Mr. Jaczewski's payments to Naicom. *Id.* ¶ 135. However, these allegations are almost entirely vague, conclusory, and devoid of factual development. At best, they describe the inner workings of the association in fact in a few isolated instances. But they fail to adequately describe how, apart from these isolated instances, the alleged association in fact 'function[ed] as an ongoing unit" or constituted an "ongoing organization" during the two-plus years it allegedly existed. *Cianci*, 378 F.3d at 82 (internal quotations omitted). In short, Plaintiffs offer virtually no well-pleaded facts explaining how the conspirators functioned together as an ongoing unit or organization.

Plaintiffs attempt to compensate for this lack of well-pleaded facts by offering that "[t]he Association-In-Fact defendants had an ongoing organizational framework

for carrying out the Racketeering Enterprises' criminal objectives" because "[t]he Association-In-Fact defendants could not have carried out the intricate task of robbing Plaintiffs' Intellectual Property and Trade Secrets . . . unless it had some structure for making and communicating group decisions." *Second Am. Compl.* ¶ 130. The Court views this allegation as the epitome of a "[t]hreadbare recital[] of the elements of a cause of action, supported by mere conclusory statements." *Iqbal*, 556 U.S. at 678. It merely restates the requirement that the enterprise have an organizational framework, supported by nothing but the circular logic that the purported enterprise could not have succeeded unless it were truly an enterprise. There is, however, an obvious alternative explanation: the DISH/NagraStar Defendants were assisting the Federal Defendants with a legitimate law enforcement investigation, not joining with them to steal Plaintiffs' intellectual property as part of an elaborate conspiracy. These allegations do not adequately plead the existence of an "ongoing unit" or "ongoing organization" required for a RICO claim. *Cianci*, 378 F.3d at 82 (internal quotations omitted)

Furthermore, "criminal actors who jointly engage in criminal conduct that amounts to a pattern of 'racketeering activity' do not automatically thereby constitute an association-in-fact RICO enterprise simply by virtue of having engaged in the joint conduct" and "[s]omething more must be found—something that distinguishes RICO enterprises from ad hoc one-time criminal ventures." *Id.*; *see also Bachman v. Bear Stearns & Co., Inc.,* 178 F.3d 930, 932 (7th Cir. 1999) (noting that a contrary rule would erroneously make "every conspiracy to commit fraud . . . a RICO [enterprise]

and consequently every fraud that requires more than one person to commit . . . a RICO violation"). While Plaintiffs assert that the DISH/NagraStar Defendants have previously been involved in trade secret misconduct,[8] *see Second Am Compl.* ¶ 129; *Pls.' Opp'n* at 4-5, they do not allege that this association in fact as a whole has engaged or will engage in any misconduct unrelated to the one-off goal of stealing Plaintiffs' intellectual property. In its review of the Second Amended Complaint, the Court is unable to find the "[s]omething more" that "must be found . . . that distinguishes RICO enterprises from ad hoc one-time criminal ventures." *Cianci*, 378 F.3d at 82.

As noted earlier, Civil RICO claims "premised on mail or wire fraud must be particularly scrutinized because of the relative ease with which a plaintiff may mold a RICO pattern from allegations that, upon closer scrutiny, do not support it." *Efron*, 223 F.3d at 20. Ultimately the Court concludes that the Second Amended Complaint, when stripped of its conclusory allegations, does not assert sufficient facts to plead the existence of a RICO enterprise, and that Plaintiffs' RICO claim must fail.

2. Pattern of Racketeering Activity

Plaintiffs must also plead a "pattern of racketeering activity," which "means the commission of at least two related acts of racketeering activity during a period of ten years." *Humana, Inc. v. Biogen, Inc.*, 666 F. Supp. 3d 135, 147 n.4 (D. Mass. 2023)

[8] This allegation is supported only by citations to other lawsuits involving the DISH/NagraStar Defendants. *See Second Am. Compl.* ¶ 129; *Pls.' Opp'n* at 4-5. Even assuming the association in fact involved only the DISH/NagraStar Defendants, which runs counter to many allegations in the Second Amended Complaint, Plaintiffs have still failed to allege how this alternative association in fact functioned as an ongoing unit.

(citing 18 U.S.C. § 1961(5)). "Racketeering activity" is defined to include a variety of predicate offenses, including mail fraud, wire fraud, and theft of trade secrets. 18 U.S.C. § 1961(1). The First Circuit has observed that the Supreme Court has found "that the civil RICO provision's 'by reason of' language contains both but-for causation and proximate causation requirements." *In re Neurontin Mktg. & Sales Pracs. Litig.*, 712 F.3d 21, 34 (1st Cir. 2013) (citing *Holmes v. Secs. Investor Prot. Corp.,* 503 U.S. 258, 268 (1992)).

Plaintiffs allege that the purported RICO conspiracy's pattern of racketeering activity involved numerous predicate acts, including:

> [A]cts indictable under Mail Fraud (18 U.S.C. § 1341), Wire Fraud (18 U.S.C. § 1343), Conspiracy to Commit Mail And Wire Fraud (18 U.S.C. § 1341), Theft Of Trade Secrets Under The Defend Trade Secrets Act (18 U.S.C. § 1836 et seq.), while in addition, committing the possible underlying criminal offenses as prohibited under [the Computer] Fraud and Abuse Act (18 U.S.C. § 1030(a)); Stored Communications Act (18 U.S.C. §§ 2701-12); Digital Millennium Copyright Act (17 U.S.C. § 1201 et seq.), 18 U.S.C.A. § 2235-Search warrant procured maliciously; 18 U.S.C.A. § 1621- Perjury generally; 18 U.S.C.A. § 1001-Statements or entries generally, 18 U.S.C.A. § 912-Officer or employee of the United States; 18 U.S.C.A. § 2234-Authority exceeded in executing warrant; 18 U.S.C.A. § 2236-Searches without warrant, 18 U.S.C.A. § 1905-Disclosure of Confidential Information, while accomplishing their racketeering objectives.

Second Am. Compl. ¶ 132.

Most of these alleged offenses are not "predicate acts" under the RICO statute. Mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), and theft of trade secrets

(18 U.S.C. §§ 1831-1832)[9] qualify; the rest do not. *See* 18 U.S.C. § 1961(1) (listing qualifying offenses).

a. Wire and Mail Fraud

"Mail or wire fraud requires proof of (1) a scheme to defraud based on false pretenses; (2) the defendant's knowing and willing participation in the scheme with the specific intent to defraud; and (3) the use of interstate mail or wire communications in furtherance of the scheme." *Sanchez v. Triple-S Mgmt., Corp.*, 492 F.3d 1, 9-10 (1st Cir. 2007). "The 'in furtherance' requirement is to be read broadly." *United States v. Simon*, 12 F.4th 1, 33 (1st Cir. 2021). "[T]he mails need not be an essential element of the scheme. It is sufficient for the mailing to be incident to an essential part of the scheme, or a step in [the] plot." *Schmuck v. United States*, 489 U.S. 705, 710-11 (1989) (second alteration in original) (internal citations and quotations omitted).

Federal Rule of Civil Procedure 9(b) requires that "[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake." FED. R. CIV. P. 9(b); *see also Humana*, 666 F. Supp. 3d at 154 ("Civil RICO claims based on the predicates of mail or wire fraud must meet the heightened pleading standard of Rule 9(b)"). A complaint must specify "the time, place, and content of an alleged false representation." *United States ex. rel. Kelly v. Novartis*

[9] The statutory provision cited by Plaintiffs—18 U.S.C. § 1836—discusses civil proceedings for misappropriation of trade secrets and is not listed as a predicate act in 18 U.S.C. § 1961(1). Since the Court assumes that Plaintiffs' reference to 18 U.S.C. § 1836 was in error, the Court has recharacterized their predicate-act allegations relating to theft of trade secrets as arising under 18 U.S.C. §§ 1831 and 1832.

Pharms. Corp., 827 F.3d 5, 13 (1st Cir. 2016) (quoting *Doyle v. Hasbro, Inc.*, 103 F.3d 186, 194 (1st Cir. 1996)). Furthermore, "[t]he false or fraudulent representation [in a mail or wire fraud claim] must be material." *United States v. Appolon*, 715 F.3d 362, 367 (1st Cir. 2013) (first alteration in original) (citation omitted).

Plaintiffs' mail and wire fraud claims are limited to allegations that Mr. Jaczewski—in an operation "instructed" by Mr. Gedeon, Mr. Smith, Mr. Eichhorn, and Ms. Rinkel and "supervised and approved" by the Federal Defendants—used an alias to purchase two Naicom set-top boxes and a monthly subscription he maintained for two years. *Second Am. Compl.* ¶¶ 132-37. In Plaintiffs' view, each purchase or payment "constitutes a wire fraud racketeering act since [Mr. Jaczewski, acting under the alias] Brian Parsons, posed as [a] legitimate client and used the interstate internet electronic services to access Naicom's website, and register online under the false pretenses of BRIAN PARSONS" and "made online payments through the use of interstate internet electronic services . . . to defraud and deprive Naicom Corporation of its legitimate products, intellectual property and trade secrets." *Id.* ¶ 134. Between the initial purchases and monthly subscription payments, Plaintiffs tally 22 acts of wire fraud. *Id.* ¶ 135. Finally, they also consider the initial purchase to constitute mail fraud because Mr. Jaczewski "posed as a legitimate client and used the United States Postal Services to have Naicom mail him the IPTV Set Top Box to a fake address." *Id.* ¶ 133.

Accepting these allegations as true, the Court concludes that the facts are insufficient to support Plaintiffs' wire and mail fraud claims because the purportedly

fraudulent representations (limited to Mr. Jaczewski's use of an alias for the set-top box purchase and subscription) were not material. Nor could the mail and wire fraud allegations be predicate acts for Plaintiffs' RICO claim because the set-top-box operation was not causally connected to Plaintiffs' damages.

A material statement "has a natural tendency to influence, or [is] capable of influencing, the decision of the decisionmaking body to which it was addressed" but plaintiffs "need not prove that the decisionmaker actually relied on the falsehood or that the falsehood led to actual damages." *Appolon*, 715 F.3d at 368 (alteration in original) (citations and internal quotation omitted). In *Appolon*, the defendant provided untrue responses on a mortgage application, in response to questions "that specifically sought information regarding the purchaser's income, assets, and intent to reside in the property." *Id.* The First Circuit considered the false responses material because the questions "were designed to assess the borrower's creditworthiness" and thus the statements "were capable of influencing [the lender's] decision." *Id.*

The purported false statements here are far afield from providing false financial information on a mortgage application. Naicom's set-top boxes are commercial electronic products sold in retail stores like Sam's Club, and its subscription services are available on Apple's AppStore as the Naicom TV App. *Second Am. Compl.* ¶ 70 ("On February 16, 2017, Apple Corporation approved Naicom Corporation App for Apple's AppStore as Naicom TV App"); *id.* ¶ 71 ("On December 15, 2017, Sam's Club approved Naicom Corporation to officially launch and

distribute in their retail stores [] Naicom's IPTV Set Top Box which offered the distribution of tv programming to customers in Puerto Rico"). Parsing Plaintiffs' allegations, they allege that Mr. Jaczewski committed wire and mail fraud by providing a false name "of BRIAN PARSONS, fake Phone (727) 409-9464, fake Email: parsons.brian716@outlook.com and Address: 9079 FOURTH STREET NORTH SAINT PETERS FL 33702 IP: 70.127.233.139, and made online payments through the use of interstate internet electronic services using the PM Visa ending in 2775." *Id.* ¶ 134. Plaintiffs also allege that Mr. Jaczewski used the alias of Brian Parsons when purchasing two Naicom set-top boxes. *Id.* ¶ 133.

The allegations confirm that Mr. Jaczewski used the false name of Brian Parsons. It is unclear, however, what Plaintiffs mean by a "fake Phone"—whether Mr. Jaczewski used a different phone as part of the alias or if the number provided was entirely made up. Plaintiffs have not adequately pleaded that the remainder of the "false" statements are actually false. The Second Amended Complaint does not allege that email services require customers to use their real name in their email address. Thus, the Second Amended Complaint fails to allege that using an email with "parsons.brian" in the address is a false statement as there is no allegation that the address itself does not actually exist. It is unclear what Plaintiffs mean by a "fake" address, but again, the Second Amended Complaint also does not allege that online retail customers are prohibited from having a product shipped to any address they desire, and Plaintiffs have offered nothing to suggest that this constitutes a false

representation.[10] Likewise, nothing in the Second Amended Complaint suggests that the IP address or credit card involved false statements.[11]

The Court is thus left to consider whether Mr. Jaczewski's purchase of two commercially available products and an accompanying subscription using the name Brian Parsons can support Plaintiffs' alleged mail and wire fraud violations. The Court concludes that it cannot, because—absent allegations to the contrary—a customer providing a false name in such circumstances does not have "a natural tendency to influence, [nor is it] capable of influencing, the decision of the decisionmaking body to which it was addressed." *Appolon*, 715 F.3d at 368. Nothing in the Second Amended Complaint suggests that the use of this alias was material to Plaintiffs' decision to sell Mr. Jaczewski their commercially available product. There is no allegation that Mr Jaczewski was either known to Plaintiffs or prohibited from purchasing Plaintiffs' products. What is missing is an allegation that the alias could have reasonably affected the "decision of the decisionmaking body" (for example, Naicom's sales department's decision to process Mr. Jaczewski's payment or ship his order). Absent allegations regarding how Mr. Jaczewski's alias affected Naicom's decision to sell him their product, Plaintiffs have not pleaded material fraud with the

[10] In theory, Mr. Jaczewski could have provided an address that was entirely made up. This seems unlikely, however, in light of the Second Amended Complaint's allegations that the Defendants used the set-top boxes to attempt remote attacks on Naicom's servers. Had the boxes been shipped to an address that didn't exist, they would have been returned to Naicom as undeliverable, meaning that the Defendants could not have used them to launch sniffing attacks. The Plaintiffs do not appear to allege that the mailing address is a fake address, and the Court doubts that they could do so, based on the information in this case.

[11] To the contrary, in the Second Amended Complaint, Plaintiffs include a table listing all the payments made to Naicom by Mr. Jaczewski posing as Brian Parsons. *Second Am. Compl.* ¶ 136. In the Court's view, these payments confirm that the credit card number provided by Mr. Jaczewski was valid.

requisite particularity. Plaintiffs' wire and mail fraud claims cannot stand and thus do not count as predicate acts in support of their RICO claim.

Furthermore, even if the Court did find the alleged representations material, Plaintiffs' claims fall short of the causation standard required for a wire or mail fraud-based RICO claim. *Neurontin*, 712 F.3d at 34 ("[T]he civil RICO provision's 'by reason of' language contains both but-for causation and proximate causation requirements" (citing *Holmes,* 503 U.S. at 268)). "The 'central question' in evaluating proximate causation in the RICO context 'is whether the alleged violation led directly to the plaintiff's injuries.'" *Sterling Suffolk Racecourse, LLC v. Wynn Resorts, Ltd.*, 990 F.3d 31, 35 (1st Cir. 2021) (quoting *Anza v. Ideal Steel Supply Corp.*, 547 U.S. 451, 461 (2006)). Quoting the U.S. Supreme Court, the First Circuit has noted that "[a] link [between the RICO predicate acts and the plaintiff's injuries] that is too remote, purely contingent, or indirect is insufficient to show proximate cause." *Id.* (alterations in original) (quoting *Hemi Grp., LLC v. City of New York*, 559 U.S. 1, 9 (2010)). In addition, the First Circuit has identified "three functional factors with which to assess whether proximate cause exists under RICO."[12] *Id.* (quoting *Neurontin*, 712 F.3d at 35-36)). The but-for causation question, in contrast, asks

[12] These factors are:

> (1) "concerns about proof" because "the less direct an injury is, the more difficult it becomes to ascertain the amount of a plaintiff's damages attributable to the violation, as distinct from other, independent, factors," . . . (2) "concerns about administrability and the avoidance of multiple recoveries," . . . and (3) "the societal interest in deterring illegal conduct and whether that interest would be served in a particular case[.]"

Sterling Suffolk Racecourse, 990 F.3d at 35-36 (quoting *Neurontin*, 712 F.3d at 35-36).

whether the plaintiff would have suffered the same injury absent the defendant's violation. *See Neurontin*, 712 F.3d at 34.

Here, the alleged violations fail both causation tests because Plaintiffs portray the set-top-box operation as an unmitigated failure that only provided further proof that Naicom was a legitimate company. They allege that "after testing Naicom TV several times to identify if it was providing DISH programming, on each case the test *revealed no DISH content*." *Second Am. Compl.* ¶ 90 (emphasis added). After attempting to use the boxes to penetrate Plaintiffs' network and steal their secrets, the "Dish/Nagrastar defendants also informed the Racketeering Enterprises that the Association in Fact defendants couldn't penetrate Naicom's Data Center computers, servers, encoders electronic security system, and that a physical intrusion was necessary to extract the intellectual property from the computers, servers, and encoders by physical access." *Id.* ¶ 93. They allege further that the operation did not yield evidence that would support a search warrant and thus the defendants had to provide "affidavits they knew contained material information known to be false and perjured to create probable cause to gain legal access into Plaintiffs['] private business." *Id.* ¶ 20.

As the Court understands the Second Amended Complaint, Plaintiffs allege that all Defendants conspired from the outset to steal their intellectual property. The set-top-box operation was an attempt to steal Plaintiffs' secrets by reverse engineering the technology and/or penetrating Plaintiffs' networks. But the operation failed. All the Defendants gained was more proof that Naicom was a

legitimate company, and they then had to resort to falsifying affidavits to justify physical access to Naicom's Data Center (through a search warrant) that would finally allow them access to the desired technology. Plaintiffs have not alleged any harm prior or unrelated to the execution of the warrants. Nor have Plaintiffs alleged that the Defendants would not have sought and executed the search warrants had they not undertaken the set-top-box operation.

The Court concludes that there is no connection—proximate or but-for—between the allegedly fraudulent set-top-box purchase and Defendants acquiring Plaintiffs' intellectual property during the execution of the warrants. The alleged mail and wire fraud is "too remote" from Plaintiffs' alleged harms, *Hemi Grp.*, 559 U.S. at 9, and there is no indication that Plaintiffs would not have suffered their alleged harms absent the set-top-box operation. Plaintiffs' Second Amended Complaint thus falls short on both the materiality and causation standards for wire and mail fraud as predicate acts.

b. Theft of Trade Secrets

Plaintiffs also plead that the Federal Defendants committed RICO predicate acts by misappropriating their trade secrets. *See Second Am. Compl.* ¶¶ 138-41. As noted above, RICO predicate offenses include any act indictable under 18 U.S.C. § 1832, relating to theft of trade secrets under the DTSA. 18 U.S.C. § 1961(1). 18 U.S.C. § 1832 provides that "[w]hoever, with intent to convert a trade secret . . . to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—steals, or

without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information," or attempts to do so, shall be subject to criminal penalties. *Id.* § 1832(a)(1), (a)(4). "Trade secret" is defined broadly to include "all forms and types of financial, business, scientific, technical, economic, or engineering information," as long as "the owner thereof has taken reasonable measures to keep such information secret" and "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information." *Id.* § 1839(3). Critically, however, the DTSA also provides that "[t]his chapter does not prohibit . . . any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State." *Id.* § 1833(a)(1).

The scope of Plaintiffs' DTSA claims is unclear. Plaintiffs generally allege that "[b]eginning on or before August 7, 2017," Mr. Gedeon, Mr. Smith, Mr. Eichhorn, and Ms. Rinkel, along with the Federal Defendants: "stole, and without authorization misappropriated, took, carried away, or by fraud, artifice, or deception obtained trade secrets," *Second Am. Compl.* ¶ 138; "did without authorization, spy, reverse engineered, copied, duplicated, downloaded, uploaded, altered, destroyed, replicated, transmitted, delivered, sent, communicated, and/or conveyed intellectual property and trade secrets," *id.* ¶ 139; and "misappropriated, obtained, or converted without authorization [the trade secrets] to the economic benefit of [the] Racketeering Enterprises and other defendant coconspirators." *Id.* ¶ 140. Additionally, the Second

Amended Complaint clearly alleges that the *Federal Defendants* violated the DTSA on August 27 and 29, 2019 (the dates of the search-warrant executions) by "facilitating and assisting" the DISH/NagraStar Defendants' entry into Naicom's facility to steal Naicom's trade secrets. *Id.* ¶ 141. However, it is unclear whether this allegation encompasses the DISH/NagraStar Defendants, as it appears to be targeted at the Federal Defendants.

The only clarity in Plaintiffs' 69-page opposition is their contention that "[t]he record also supports the finding that the Dish/Nagrastar defendants' misappropriations of Plaintiffs' trade secrets by illegal means is unlawful given the way Dish/Nagrastar defendants obtained the same through the illegal search warrant, warrantless executions, and trespass." *Pls.' Opp'n* at 68. Based on the content of Plaintiffs' Second Amended Complaint and their statements in opposition to the DISH/NagraStar Defendants' motion to dismiss, the Court narrows the scope of the DTSA inquiry to the DISH/NagraStar Defendants' actions related to obtaining and executing the search warrants—discarding any other DTSA allegations as pleaded with insufficient particularity.

The DISH/NagraStar Defendants dispute Plaintiffs' misappropriation of trade secrets claim by arguing that their conduct was "supported by allegations of legitimate government action."[13] *Defs.' Mot.* at 9 (quoting *Kahre v. Damm*, No. 2:07-CV-00231-DAE-RJJ, 2007 U.S. Dist. LEXIS 95978, at *26 (D. Nev. Dec. 18, 2007)).

[13] Here, the Court is quoting from the section of the motion that argues the DISH/NagraStar Defendants lacked the requisite criminal intent for liability under RICO. However, from the Court's perspective, these arguments apply with equal force here because the reason the Defendants lacked criminal intent was that they were acting pursuant to warrants.

They further submit that "as private individuals enlisted by the Federal Defendants, 'acting as federal agents' under color of federal law at the direction of and in conjunction with the Federal Defendants, to assist in discharging essential government activities, including the . . . execution of the search warrants, the DISH/NagraStar Defendants are not subject to liability under RICO." *Id.* at 11.

In response, Plaintiffs argue that the "procurement of the issuance and execution of the search and seizure warrant and the subsequent warrantless search and seizure execution were illegal and unconstitutional." *Pls.' Opp'n* at 18. Because Plaintiffs' misappropriation claims center on the execution of the warrants, and they dispute the validity of the warrants, the Court addresses this issue first.

As a threshold matter, the Court addresses whether the DISH/NagraStar Defendants, as private parties, can justify their actions based on the search warrants. The DISH/NagraStar Defendants submit that their "aiding the Federal Defendants in their execution of search warrants" does not "render the warrants invalid or constitute illegal trespass, as federal law authorizes government officials to procure assistance from private individuals in aid of a search warrant's execution." *Defs.' Mot.* at 9-10. Plaintiffs concede that "[f]ederal constitutional law does not proscribe the use of civilians in searches," and "[c]ourts have recently upheld the practice." *Pls.' Opp'n* at 26-27. They counter, however, that the search warrants here were issued and executed illegally because 1) 18 U.S.C. § 3105 "clearly prohibit[s] the executing officer from bringing to the search a party which had another interest, profit, or other marketplace incentive," 2) the government did not "seek authorization from the

Magistrate to bring Plaintiffs' competitors," and 3) "the Dish/Nagrastar defendants were executing the search warrant on their own, as they wanted." *Id.* at 28-29. None of Plaintiffs' arguments has merit.

As Plaintiffs concede, federal law allows private parties to assist in the execution of search warrants. 18 U.S.C. § 3105 provides, in its entirety:

> A search warrant may in all cases be served by any of the officers mentioned in its direction or by an officer authorized by law to serve such a warrant, but by no other person, except in aid of the officer on his requiring it, he being present and acting in its execution.

On its face, the statute allows private parties to assist in the execution of search warrants "in aid of the officer on his requiring it." *Id.*

Plaintiffs contend that 18 U.S.C. § 3105 "clearly prohibit[s]" officers from being assisted by private parties with economic interests adverse to those of a search warrant's target. *Id.* at 29. But the statute does not mention such a prohibition. Further, since the statute allows private-party assistance, enlisting the DISH/NagraStar Defendants may well have been desirable in this case, given the specialized, technical nature of the evidence sought by investigators. *See generally Pls.' Opp'n*, Attach 1. at 272-94, *Aff. in Supp. of an Application for a Search Warrant* (*Warrant Aff.*). Notwithstanding Plaintiffs' insistence to the contrary, the Federal Defendants' decision to enlist the DISN/NagraStar Defendants strikes the Court as reasonable, given the DISH/NagraStar Defendants' likely familiarity with evidence of digital piracy.

Plaintiffs also maintain that the First Circuit, in *Bellville v. Town of Northboro*, 375 F.3d 25 (1st Cir. 2004), announced a rule that any private-party

assistance must be authorized by a magistrate judge. *Pls.' Opp'n* at 27-29. This arguments rests on a misreading of *Bellville*. In *Bellville*, the First Circuit noted that there was *no* authority for a rule requiring magistrate approval for private-party assistance and therefore declined to impose such a rule. *Bellville*, 375 F.3d at 33. The First Circuit did observe that "it might be a 'better practice,' if circumstances permit, for law enforcement officers to disclose to the magistrate that civilians will be involved in the execution of the search and for the warrant to indicate that the magistrate permitted this involvement." *Id.* at 34. But a best practice is not a rule, and the Court declines Plaintiffs' invitation to make the best practice outlined in *Bellville* binding on law enforcement.

Finally, Plaintiffs suggest that the DISH/NagraStar Defendants cannot rely on the warrants because "[t]he evidence collected in this case clearly demonstrates that the Dish/Nagrastar defendants were executing the search warrant on their own, and as they wanted." *Pls.' Opp'n* at 29. From a factual perspective, this contention is inconsistent with the allegations in the Second Amended Complaint. *See Second Am. Compl.* ¶¶ 21-22 (noting the DISH/NagraStar Defendants were "acting as federal agents"); *id.* ¶ 106 (noting that, during the August 29, 2019 search, the FBI Defendants gave Mr. Smith, Mr. Gedeon, and Mr. Eichhorn "permission to penetrate Naicom's Data Center and introduce pen drives"). Further, even assuming the DISH/NagraStar Defendants were executing the searches without supervision, that alone does not invalidate the searches. *See Bellville*, 375 F.3d at 34 ("[T]he Fourth Amendment does not explicitly require official presence during a warrant's execution,

therefore it is not an automatic violation if no officer is present during a search" (quoting *United States v. Bach*, 310 F.3d 1063, 1066-67 (8th Cir. 2002))). Other than the wholly conclusory allegation that the DISH/NagraStar Defendants were executing the search warrants "as they wanted," Plaintiffs make no allegation that the DISH/NagraStar Defendants did "anything that [they] would not have done if [the Federal Defendants] had been in the room." *See id.*

In short, then, Plaintiffs' arguments that the search warrants were invalid because of the involvement of the DISH/NagraStar Defendants are all unavailing. The Second Amended Complaint clearly alleges, multiple times, that the DISH/NagraStar Defendants were "acting as federal agents" while assisting with the execution of the search warrants. Because such assistance was legally permissible, the Court concludes that the DISH/NagraStar Defendants are able to rely on the search warrants in defending against Plaintiffs' misappropriation claims. Thus, the key question becomes whether the warrants themselves were valid.

The relevant standard for evaluating the validity of a warrant is the *Franks v. Delaware* framework, which requires Plaintiffs to adequately allege that both (1) "a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit" and (2) "the allegedly false statement is necessary to the finding of probable cause." *United States v. Reiner*, 500 F.3d 10, 14 (1st Cir. 2007) (quoting *Franks v. Delaware,* 438 U.S. 154, 155-56 (1978)). Plaintiffs cite ten statements that they allege the Defendants "falsely submitted to

the Court" in an affidavit supporting their search-warrant application. *Pls.' Opp'n* at 19. The Court has examined each and concludes that none supports Plaintiffs' claims.

The first purportedly false statement identified by Plaintiffs is the Defendants' statement that they believed there was probable cause that Plaintiffs were violating copyright and money laundering laws. *Id.* Plaintiffs allege that this statement is false because:

> The execution of the search and seizure warrant in this case did not produce any criminal evidence whatsoever; there was no probable cause. That is why the United States never opposed Plaintiffs[']s Motion for Return of Property under Rule 41(g) of the Fed.R.Crim.P. In fact, they didn't even contend the serious violations Plaintiffs imputed under *Franks* in the Rule 41(g) motion.

Id. This logic is unavailing. Plaintiffs cannot rely on the circular reasoning that the search's alleged failure to produce incriminating evidence thereby proves the Defendants could not have believed there was probable cause to search. *See Karamanoglu v. Town of Yarmouth*, 15 F.4th 82, 88 (1st Cir. 2021) (defining the probable cause inquiry as "whether, on balance, the facts *known to the officer at the time of the arrest* support probable cause" (emphasis in original)).

Equally inadequate is Plaintiffs' claim that the Federal Defendants' failure to oppose Plaintiffs' motion to return the seized property proves not only that the seized property was not incriminating, but also that there was no probable cause to search in the first place. *See United States v. Pierre*, 484 F.3d 75, 87 (1st Cir. 2007) ("Once seized property is no longer needed as evidence, a criminal defendant is presumed to have the right to its return"). The government's return of the seized hard drives and

thumb drives, which—unlike drugs or illegal firearms—are not inherently contraband and can easily be downloaded or duplicated, is consistent with *Pierre*.

Furthermore, Plaintiffs are simply incorrect that success on a Rule 41(g) motion conclusively establishes the invalidity of a search. Rule 41(g) allows motions for return of property from "[a] person aggrieved by an unlawful search and seizure of property *or* by the deprivation of property." FED. R. CRIM. P. 41(g) (emphasis supplied). Without more, the property's return alone cannot demonstrate an absence of probable cause to search and seize in the first place. Ultimately, Plaintiffs' first purportedly false statement offers nothing to undermine the validity of the warrants and searches.

Second, Plaintiffs offer that the Defendants "assured the Court they had evidence based on an investigation conducted by Nagrastar of Naicom's unauthorized use of Direct TV signal to distribute its programming to its paid subscribers." *Pls.' Opp'n* at 19. Plaintiffs assert that this statement was false because "[t]he United States did not produce any evidence as to the above allegations," whereas "Naicom did produce all the documentary evidence establishing that they were authorized to distribute the copyright material and running a legitimate IPTV system." *Id.*

Again, Plaintiffs appear to be suggesting that exculpatory evidence they produced during the search proves that the affidavit was false. These conclusory assertions tied together by circular logic do not adequately demonstrate the falsity of the affidavit. While Plaintiffs contend that the affidavit did not "produce any evidence" supporting the suggestion that Naicom was distributing DirecTV content

without authorization, the affidavit avers that Naicom's system displayed DirecTV error messages on at least 16 channels (and includes a photo of the message), that Naicom's satellite dishes were precisely oriented in a manner necessary to receive DirecTV satellite signals, that representatives of the companies offering some channels Naicom purported to provide confirmed that Naicom was not licensed to provide them, and other indicia of piracy. *See Warrant Aff.* Simply put, Plaintiffs' argument that the affidavit contained no evidence of piracy is incorrect.

Third, Plaintiffs assert that, during a 2018 FBI site visit of Naicom's property, Mr. Vega "repeatedly told the agent that Naicom was a legal corporation and showed the agent a certificate from the National Cable Television Cooperative (NCTC) on the wall," yet the Federal Defendants still "filed the affidavit containing materially false and perjured statements." *Pls.' Opp'n* at 19-20. It is not clear specifically which "materially false and perjured statements" Plaintiffs are referring to, but the affidavit states that the FBI called NCTC's management group, which confirmed that Naicom was *not* a member. *Warrant Aff.* ¶ 15. Nothing in Plaintiffs' assertion that Mr. Vega told the FBI his company was legitimate and showed them a certificate on the wall establishes that the affidavit's claim—that NCTC management represented to the FBI that Naicom was not a member—was perjured.

Fourth, Plaintiffs contend that the affidavit's claim that Naicom was using the NCTC certificate to create the appearance of legal access to channels was a "false and perjured statement" because an FBI agent took pictures of "Naicom's National Rural

Telecommunications Cooperative 'NRCT' Certificate" and Naicom had licenses with other networks. *Pls.' Opp'n* at 20.

Fifth, Plaintiffs focus on the affidavit's claim that an FBI agent spoke with NCTC management, who confirmed that Naicom was not a member of their organization. *Id.* They allege that this "is a false and perjured statement" because Naicom provided evidence that it is a member of the NRTC. *Id.*

The distinction between NCTC and NRTC here is somewhat confusing. It appears that Plaintiffs are alleging that the FBI took pictures of a NRTC certificate on the wall but incorrectly referred to it in the affidavit as a NCTC certificate, or that the FBI mistook their NRTC certificate for an NCTC certificate. However, Plaintiffs also claim that the affidavit's assertion that they are not a member of the NCTC is a perjured statement because they provided evidence that they are a member of the NRTC. Plaintiffs offer no evidence that the latter statement was perjured because proving they are a NRTC member does not contradict the claim that they are not a NCTC member. To the extent that the FBI may have misidentified a NRTC certificate as a NCTC certificate, the record does not suggest that this "allegedly false statement is necessary to the finding of probable cause," especially given the strength of the other supporting claims in the affidavit. *United States v. Patterson*, 877 F.3d 419, 424 (1st Cir. 2017) (quoting *Franks*, 438 U.S. at 156).

Sixth, Plaintiffs turn to the affidavit's assertion that FBI agents contacted officials at HBO and DirecTV, who verified that Naicom did not have a relationship with their organizations despite offering HBO content. *Pls.' Opp'n* at 20-21.

Plaintiffs claim that "[t]his is a false and perjured statement" because "Naicom provided evidence that it is licensed to distribute HBO and Cinemax programming." *Id.* at 21 (citing *Pls.' Opp'n*, Attach. 1 at 356 (HBO invoice dated August 31, 2019, for roughly $200 per month for "Cable — Private Home" services)). Plaintiffs' claim is unpersuasive for two reasons: (1) this invoice for inexpensive "Cable – Private Home" services does not appear to provide evidence of a licensing agreement; and (2) Plaintiffs have not directly contradicted the purportedly perjured claim, which was that HBO and DirecTV officials represented to the FBI that they did not have a relationship with Naicom.

Seventh, Plaintiffs focus on the affidavit's claim that the "external appearance of the Data Center offered indicia of piracy," calling it a "false and perjured statement" because "[a]t the conclusion of the search and seizure warrant execution the FBI agents found that [] Naicom's equipment (encoders) were provided by the networks authorizing the programming distribution and that the use of the satellite was in fact to download the codes provided by the networks." *Pls.' Opp'n* at 21. Plaintiffs again rely on circular logic, as the discovery of exculpatory evidence at the conclusion of a warrant's execution does not provide a "substantial preliminary showing" that the underlying affidavit was perjured. *Franks*, 438 U.S. at 155-56.

Plaintiffs' eighth point suffers from the same defect. They claim that the affidavit's statements that there were suspicious financial transactions between Naicom and other businesses owned by Mr. Quinones and Mr. Vega were false and perjured because "[d]uring the execution of the Search Warrant S/A Lange

interviewed employees from the Business Office and was provided with financial records," which established "that none of the Corporations were involved in any money laundering activities." *Pls.' Opp'n* at 21-22. Again, the fact that a search did not uncover incriminating evidence does not establish that it was predicated on a perjured affidavit.

Plaintiffs' ninth point takes issue with the affidavit's request to seize computers and data based on claimed probable cause that they contained evidence. *Id.* at 22. Plaintiffs contend that this statement was perjured because "the FBI agents were not looking for any criminal evidence" during the search and they did "not find[] any evidence whatsoever of the crimes described in the warrant, which also denied any probable cause." *Id.* The Court does not fully follow Plaintiffs' logic across these seemingly contradictory assertions, but they appear to use the same circular reasoning (the assertion of probable cause was perjured because the resulting search "denied any probable cause"), along with the conclusory contention that the FBI was not actually looking for evidence. These claims do not undermine the validity of the warrants.

Tenth, Plaintiffs claim that the affidavit's request to seize evidence relating to statutory violations was "false and perjured" because the FBI did not find any evidence at the conclusion of the search-warrant execution. *Id.* Beyond the fact that this argument relies on the same circular logic, an affidavit's request to seize "things and . . . records" is not an assertion of fact and cannot be false or perjured. *Id.*

To summarize, none of these purportedly false statements, alone or in combination, satisfies Plaintiffs' burden under the *Franks* standard to overcome the presumed validity of the warrants. Moreover, Plaintiffs offer several additional arguments that are similarly unavailing.

Plaintiffs submit that the August 29, 2019 search was "illegal" and "warrantless" because "[t]he Federal and Dish/Nagrastar defendants knew for a fact that the first search warrant execution had already denied any criminal wrongdoing, and that the initial alleged probable cause had dissipated." *Id.* at 29. This assertion—that the Defendants knew probable cause had dissipated—is wholly conclusory (especially in light of Plaintiffs' argument that the entire investigation was a hoax, and the agents knew probable cause never existed). Furthermore, the warrant did not expire until September 4, 2019 and courts generally recognize a "reasonable continuation rule" providing that a search may be reasonably continued if the warrant remains valid.[14] *See United States v. Keszthelyi*, 308 F.3d 557, 568-569 (6th Cir. 2002) (describing the rule and collecting cases). Plaintiffs have not offered any well-pleaded, nonconclusory allegations suggesting that the continuance here was unreasonable.[15]

---

[14] The "reasonable continuation rule" requires the satisfaction of two conditions: 1) "the subsequent entry must indeed be a continuation of the original search, and not a new and separate search"; and 2) "the decision to conduct a second entry to continue the search must be reasonable under the totality of the circumstances." *Keszthelyi*, 308 F.3d at 569.

[15] The closest Plaintiffs come to a nonconclusory allegation is their assertion that U.S. Attorney Rodriguez-Velez and Assistant U.S. Attorney Capo-Iriarte learned, after the execution of the first search warrant, that Naicom complied with "all the programming distribution contract and agreements." *Second Am. Compl.* ¶ 103. But this allegation is still conclusory, and it is undercut by the sentence immediately following it, which alleges that the USAO Defendants instructed S/A Pearson "to order Darwin Quinones and Victor Vega to report to the FBI Offices in San Juan with the

Plaintiffs also contend that the searches were unlawful because the Federal Defendants did not follow the procedure to obtain a Stored Communications Act warrant (also known as an SCA order). *Pls.' Opp'n* at 24-26. But this argument lacks merit because the Federal Defendants appropriately obtained a traditional search warrant in lieu of an SCA order.

SCA orders are different from traditional search warrants. As one court has explained:

> SCA warrants "are not like the search warrants used in the physical world: they are 'executed' when a law enforcement agent delivers (sometimes by fax) the warrant to the [service provider]. The [service provider], not the agent, performs the 'search'; the [service provider] 'produces' the relevant material to the agent; the user associated with the inbox often never learns that his inbox has been 'searched.' In sum, these are not search warrants at all and to call them such confuses legal terminology."

In re Info. Associated with @gmail.com, No. 16-mj-00757 (BAH), 2017 U.S. Dist. LEXIS 130153, at *52-53 (D.D.C. July 31, 2017) (quoting Paul K. Ohm, *Parallel–Effect Statutes and E–Mail "Warrants": Reframing the Internet Surveillance Debate*, 72 GEO. WASH. L. REV. 1599, 1610-11 (2004)). Additionally, the standard for an SCA order is "less stringent than the probable cause standard generally required for a search warrant." *United States v. Taylor*, 54 F.4th 795, 804 (4th Cir. 2022). Finally, even if the Federal Defendants were seeking information protected by the SCA, the statute gives them the option of seeking either an SCA order or a traditional search

licensing contracts for an interview regarding Naicom's company." *Id.* Clearly, whatever U.S Attorney Rodriguez-Velez and Assistant U.S. Attorney Capo-Iriarte learned did not absolve Naicom of wrongdoing; otherwise, there would have been no need to conduct an interview.

warrant.[16] *See* 18 U.S.C. § 2703(b) (the government may obtain "a court order for such disclosure under subsection (d) of this section" *or* "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure"); *id.* § 2703(c) (same).

Plaintiffs' argument is groundless because the Federal Defendants were primarily—if not entirely—seeking information not protected by the SCA. Regardless, they obtained search warrants for the facility and computer systems, thereby satisfying the requirements of the SCA.

Finally, Plaintiffs submit once again that "[t]he Dish/Nagrastar defendants can't raise at this time the defense that the execution of the search and seizure warrant was authorized, legal and constitutional, which was waived during the Rule 41(g) proceedings, and abandoned forever." *Pls.' Opp'n* at 32. However, as the Court has already explained, the government's decision not to oppose a motion to return property does not affect the validity of the warrant or seizure. *See Pierre*, 484 F.3d at 87 ("Once seized property is no longer needed as evidence, a criminal defendant is presumed to have the right to its return").

In sum, Plaintiffs have failed to adequately challenge the validity of the search warrants or establish that any DISH/NagraStar Defendant impermissibly assisted in the warrants' execution. Plaintiffs have thus failed to plead a DTSA violation as a predicate act in support of their RICO claim. *See* 18 U.S.C. § 1833(a)(1) ("This chapter does not prohibit . . . any otherwise lawful activity conducted by a governmental

[16] Further, "the statute offers no express direction as to when the government should seek a warrant versus" a SCA order. *Taylor*, 54 F.4th at 804.

entity of the United States, a State, or a political subdivision of a State"). Absent both an enterprise and a pattern of racketeering activity, Plaintiffs' RICO claim must be dismissed as to the DISH/NagraStar Defendants.

These same pleading shortfalls doom Plaintiffs' RICO conspiracy claim. *See Efron*, 223 F.3d at 21 (1st Cir. 2000) ("A conspiracy claim under section 1962(d) may survive a *factfinder's* conclusion that there is insufficient evidence to prove a RICO violation, but if the pleadings do not state a substantive RICO claim upon which relief may be granted, then the conspiracy claim also fails" (citations omitted) (emphasis in original)); *see also Salinas v. United States*, 522 U.S. 52, 64 (1997) ("A conspirator must intend to further an endeavor which, if completed, *would satisfy all of the elements of a substantive criminal offense*, but it suffices that he adopt the goal of furthering or facilitating the criminal endeavor" (emphasis supplied)). The Court therefore dismisses Plaintiffs' RICO conspiracy claim.

C. Plaintiffs' DTSA, CFAA, SCA, and DMCA Claims

The Court's determination that the DISH/NagraStar Defendants' conduct was authorized by valid search warrants is ultimately also fatal to Plaintiffs' DTSA, CFAA, SCA, and DMCA claims, because each statute has a similar exception for law enforcement activity.

1. The DTSA Claim

Plaintiffs' freestanding DTSA claim alleges the same violation as the DTSA claim offered as a predicate act for the RICO claim, and thus fails for the reasons previously described. While the DTSA does provide a private right of action for

owners "of a trade secret that is misappropriated . . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce," 18 U.S.C. § 1836, this right of action cannot be used to challenge "otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State." *Id.* § 1833(a)(1). The Court dismisses Plaintiffs' DTSA claim.

2. The CFAA Claim

The CFAA contains virtually the same exception for law enforcement activity. *Compare* 18 U.S.C. § 1833(a)(1) (the DTSA "does not prohibit or create a private right of action for any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State"), *with id.* § 1030(f) (the CFAA "does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States"). In *Smith v. Aldridge*, the plaintiff "allege[d] that Defendant stole his smartphone, which is legally protected under CFAA" but also admitted "that Defendant had a warrant when she accessed his phone." *Smith v. Aldridge*, No. 3:17-cv-01485-HZ, 2018 U.S. Dist. LEXIS 47021, at *18 (D. Or. Mar. 22, 2018). The district judge observed that "Defendant, therefore, had legal authority to access Plaintiff's phone at the time that she did" and because "Plaintiff admits that Defendant had a warrant, [and] Plaintiff would have to show that the warrant was invalid in order to show that the access was unauthorized . . .. [For the plaintiff] to prevail on this CFAA claim, the Court would

have to determine that Plaintiff's Fourth Amendment Rights were violated." *Id.* at *18 & n.4.

Because the DISH/NagraStar Defendants' challenged conduct was "lawfully authorized investigative . . . activity" under the search warrants, Plaintiffs have not pleaded a viable CFAA claim.[17]

3. The SCA Claim

Turning to the SCA claim, "courts in the First Circuit have consistently applied CFAA caselaw in analyzing the SCA. . .. Thus, the Court's analysis under this statute is the same as under the CFAA." *Sun West Mortg. Co. v. Flores*, No. 15-1082 (GAG), 2016 U.S. Dist. LEXIS 31149, at *11 (D.P.R. Mar. 10, 2016) (citation omitted); *see also Cheng v. Romo*, No. 11-10007-DJC, 2012 U.S. Dist. LEXIS 169535, at *10 (D. Mass. Nov. 28, 2012) ("Other district courts within this Circuit have addressed 'access without authorization' and 'exceeding authorization' in considering the analogous provision of the CFAA"). As the Court noted previously, even if the DISH/NagraStar Defendants were helping the Federal Defendants search for information protected by the SCA, the statute gives them an option of seeking either an SCA order or a traditional search warrant. *See* 18 U.S.C. § 2703(b) (the government may obtain "a court order for such disclosure under subsection (d) of this section" *or* "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure");

[17] Plaintiffs cannot avoid this result by insisting that the DISH/NagraStar Defendants were only assisting the Federal Defendants so that they could steal Plaintiffs' intellectual property. The relevant inquiry is whether the DISH/NagraStar Defendants had authorization to access the information, not whether they harbored ill motives. *See Van Buren v. United States*, 141 S. Ct. 1648, 1652 (2021) (holding that the CFAA "does not cover those who . . . have improper motives for obtaining information that is otherwise available to them").

id. § 2703(c) (same). Furthermore, even if the warrants were not valid, the SCA still provides that "[a] good faith reliance on . . . a court warrant or order . . . is a complete defense to any civil or criminal action brought under this chapter or any other law." *Id.* § 2707(e).

Even if the Court were to assume that the Federal Defendants and the DISH/NagraStar Defendants seized electronic communications protected by the SCA, they did so pursuant to valid warrants and thus did not violate the statute. Furthermore, even if the warrants were not valid, Plaintiffs' allegations of bad faith are conclusory and the Defendants would thus still be protected by the good faith defense. *See John K. MacIver Inst. for Pub. Pol'y, Inc. v. Schmitz*, 243 F. Supp. 3d 1028, 1035 (W.D. Wis. 2017), *aff'd*, 885 F.3d 1004 (7th Cir. 2018) ("Given the absence of any case law even suggesting that a state search warrant issued under similar circumstances may be invalid under the SCA, plaintiff's conclusory allegation of a lack of good faith is also wholly insufficient to support a claim that defendants 'actually knew that the [warrant] was invalid [under the SCA]'" (emphasis omitted) (alterations in original) (quoting *Sams v. Yahoo! Inc.*, 713 F.3d 1175, 1181 (9th Cir. 2013))). Plaintiffs' SCA claim will not lie against the DISH/NagraStar Defendants for essentially the same reasons as their CFAA claim.

4. The DMCA Claim

Similarly, the DMCA explicitly provides that it "does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision

of a State." 17 U.S.C. § 1201(e). This language is virtually identical to the CFAA's law enforcement exception. *Cf.* 18 U.S.C. § 1030(f) (the CFAA "does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State"). This provision of the DMCA has been interpreted as "broadly exempting official law enforcement activity." *Green v. U.S. Dep't of Just.*, 392 F. Supp. 3d 68, 77 (D.D.C. 2019).

As with the DTSA, CFAA, and SCA claims, even assuming Plaintiffs had established all the other elements of a DMCA claim, their claim would still be stymied by the statute's law enforcement exception. Plaintiffs' DTSA, CFAA, SCA, and DMCA claims all fail as pleaded because the challenged searches were conducted pursuant to lawfully authorized warrants.

D. Plaintiffs' PTSA Claim

Finally, Plaintiffs' PTSA claim fails for substantially the same reasons as their CFAA, SCA, DMCA, and DTSA claims. The PTSA provides that "[a]ny natural or juridical person who misappropriates a trade secret shall be held accountable for any damages caused to its owner." P.R. LAWS ANN. tit. 10, § 4134. Relevant here, the PTSA defines "misappropriation" as:

> (a) The acquisition of a trade secret belonging to another by a person who knew or should have known that he/she acquired such secret directly or indirectly through improper means, or
> (b) the disclosure or use of a trade secret belonging to another without his/her express or implicit consent, by a person who:
>
> (1) Used improper means to gain knowledge of the trade secret, or

> (2) at the time of disclosure or use, such person knew or should have known that such trade secret was:
>
> (A) Obtained through a person who acquired such information through the use of improper means;
>
> (B) obtained under circumstances from which a duty to maintain confidentiality or to limit use ensues;
>
> (C) obtained through a person who had the duty-bound to the trade secret's owner to maintain confidentiality or limit use, or
>
> (D) known by accident or by mistake.

Id. The PTSA further defines "improper means" as "[u]nlawful means not allowed under the law or which is contrary to free competition and to laws and regulations in effect, whereby a trade secret is obtained, including, but not limited to, misappropriation, theft, bribery, malfeasance, deceit, breach of contractual duties, wiretapping, or espionage through electronic or other means." *Id.* § 4131.

Like their DTSA claim, Plaintiffs' PTSA claim is not a picture of clarity. Plaintiffs allege that the DISH/NagraStar Defendants "misappropriated" and "exfiltrated" their trade secrets from Naicom's computer system, *Second Am. Compl.* ¶ 197, and that "[e]ach Defendant disclosed, received, and used these misappropriated trade secrets without Plaintiffs' consent, knowing or having reason to know that the trade secrets were acquired by improper means." *Id.* ¶ 199. In opposing the DISH/NagraStar Defendants' motion to dismiss, Plaintiffs represent that the "elements for a misappropriation claim" under the PTSA "are fundamentally the same" as those for a DTSA claim. *Pls.' Opp'n* at 64-65. After parsing the language in the Second Amended Complaint and taking into account Plaintiffs' equation of the DTSA with the PTSA, the Court narrows Plaintiffs' PTSA claim to cover only the

DISH/NagraStar Defendants' actions in conjunction with the search-warrant execution and discards all other allegations as insufficiently pleaded.

Plaintiffs' allegations related to the search-warrant executions are insufficient to state a claim for relief under the PTSA. As noted above, "misappropriation" under the PTSA requires the use of "improper means," which are "means not allowed under the law." But the DISH/NagraStar Defendants' conduct was "allowed under the law," as they were assisting the Federal Defendants with the execution of valid search warrants. Since Plaintiffs are unable to overcome the validity of the search warrants, they cannot show that they are entitled to relief under the PTSA. Therefore, the Court dismisses this claim as well.

VI. CONCLUSION

The Court GRANTS DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel and Jordan Smith's Motion to Dismiss (ECF No. 134). The Court DISMISSES Counts I through VII of the Second Amended Complaint as pleaded against the DISH/NagraStar Defendants.

SO ORDERED.

/s/ John A. Woodcock, Jr.
JOHN A. WOODCOCK, JR.
UNITED STATES DISTRICT JUDGE

Dated this 29th day of March, 2024